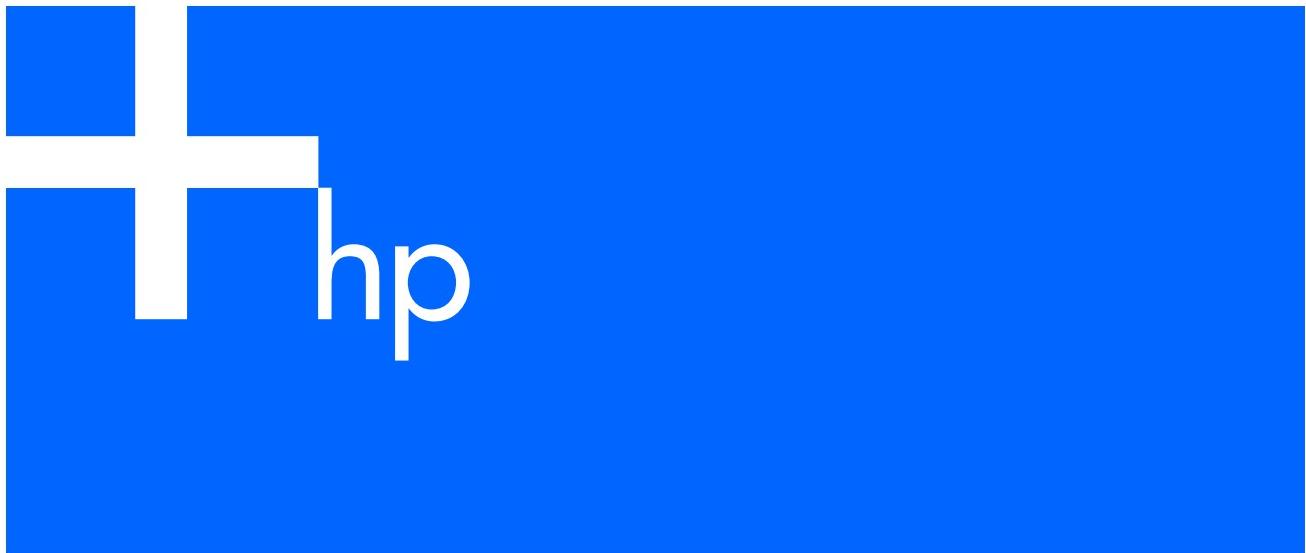


# HP ProLiant BL p-Class GbE2 Interconnect Switch Application Guide



Part number: 331403-008

Eighth edition: March 2007



## **Legal notices**

© 2004, 2007 Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft®, Windows® and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

SunOS™ and Solaris™ are trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Cisco® is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

Part number: 331403-008

Eighth edition: March 2007

# Contents

## Accessing the GbE2 Interconnect Switch

Introduction .....	8
Additional references .....	8
Typographical conventions.....	9
Using the command line interface .....	9
Connecting through the console port.....	9
Configuring an IP interface.....	9
Connecting via Telnet .....	10
Connecting via Secure Shell .....	10
Using the Browser-based Interface.....	10
Using Simple Network Management Protocol .....	11
SNMP v1.0.....	11
SNMP v3.0.....	11
Default configuration .....	12
User configuration.....	12
View based configurations .....	13
Configuring SNMP trap hosts .....	14
SNMPv2 trap host configuration .....	15
SNMPv3 trap host configuration .....	15
Secure access to the switch .....	16
Setting allowable source IP address ranges .....	16
RADIUS authentication and authorization.....	16
TACACS+ authentication .....	21
How TACACS+ authentication works.....	21
TACACS+ authentication features in GbE2 Interconnect Switch.....	21
Authorization.....	21
Accounting.....	22
Configuring TACACS+ authentication on the switch (CLI example) .....	22
Configuring TACACS+ authentication on the switch (BBI example) .....	24
Secure Shell and Secure Copy.....	25
User access control .....	29
Setting up user IDs .....	29

## Ports and trunking

Introduction .....	30
Ports on the GbE2 Interconnect Switch.....	30
Port trunk groups.....	31
Statistical load distribution.....	31
Built-in fault tolerance .....	31
Before you configure trunks .....	31
Trunk group configuration rules.....	32
Port trunking example.....	32
Configuring trunk groups (CLI example) .....	33
Configuring trunk groups (BBI example) .....	34
Configurable Trunk Hash algorithm .....	37
Link Aggregation Control Protocol.....	37
Configuring LACP .....	38

## Port-based Network Access and traffic control

Port-based Network Access control.....	40
Extensible authentication protocol over LAN .....	40
802.1x authentication process.....	40
EAPol Message Exchange .....	41
802.1x port states.....	42

Supported RADIUS attributes .....	42
EAPOL configuration guidelines .....	43
Port-based traffic control .....	43
<b>VLANs</b>	
Introduction .....	45
Overview .....	45
VLANs and port VLAN ID numbers .....	45
VLAN numbers .....	45
PVID numbers .....	45
Viewing and configuring PVIDs.....	46
VLAN tagging .....	46
VLANs and IP interfaces.....	49
VLAN topologies and design considerations .....	49
VLAN configuration rules .....	49
Multiple VLANs with tagging .....	49
Configuring the example network.....	51
FDB static entries.....	56
Trunking support for FDB static entries.....	56
Configuring a static FDB entry .....	56
<b>Spanning Tree Protocol</b>	
Introduction .....	57
Overview .....	57
Bridge Protocol Data Units .....	57
Determining the path for forwarding BPDUs.....	57
Spanning Tree Group configuration guidelines .....	58
Default Spanning Tree configuration .....	58
Adding a VLAN to a Spanning Tree Group .....	58
Creating a VLAN .....	58
Rules for VLAN tagged ports.....	58
Adding and removing ports from STGs .....	59
Assigning cost to ports and trunk groups .....	59
Multiple Spanning Trees .....	59
Why do we need Multiple Spanning Trees? .....	59
VLAN participation in Spanning Tree Groups .....	60
Configuring Multiple Spanning Tree Groups .....	60
Port Fast Forwarding .....	62
Configuring Port Fast Forwarding .....	63
Fast Uplink Convergence .....	63
Configuration guidelines .....	63
Configuring Fast Uplink Convergence .....	63
Hot Links.....	63
Forward Delay.....	63
Pre-emption .....	64
FDB Update.....	64
Configuration Guidelines .....	64
Configuring Hot Links .....	64
<b>RSTP and MSTP</b>	
Introduction .....	65
Rapid Spanning Tree Protocol.....	65
Port state changes .....	65
Port type and link type .....	65
RSTP configuration guidelines .....	66
RSTP configuration example .....	66
Multiple Spanning Tree Protocol.....	68
MSTP region.....	68
Common Internal Spanning Tree .....	68

MSTP configuration guidelines .....	68
MSTP configuration example .....	68
<b>Quality of Service</b>	
Introduction .....	73
Overview .....	73
Using ACL filters .....	74
Summary of packet classifiers .....	74
Summary of ACL actions .....	75
Using ACL Blocks and ACL Groups .....	75
Port-Based QoS actions.....	77
Metering .....	77
Re-marking .....	77
Viewing ACL statistics.....	77
ACL configuration examples.....	78
Configure Access Control Lists (CLI example) .....	78
Configure Access Control Lists and Groups (BBI example 1) .....	79
Using DSCP values to provide QoS .....	82
Differentiated Services concepts .....	83
QoS levels .....	83
Using 802.1p priorities to provide QoS.....	83
802.1p configuration (CLI example) .....	84
802.1p configuration (BBI example) .....	85
Queuing and scheduling.....	89
<b>Basic IP routing</b>	
IP routing benefits .....	90
Routing between IP subnets .....	90
Example of subnet routing .....	92
Using VLANs to segregate broadcast domains.....	93
Dynamic Host Configuration Protocol .....	95
DHCP relay agent .....	95
DHCP relay agent configuration.....	96
<b>Routing Information Protocol</b>	
Distance vector protocol.....	97
Stability .....	97
Routing updates.....	97
RIPv1 .....	97
RIPv2 .....	97
RIPv2 in RIPv1 compatibility mode.....	98
RIP Features.....	98
Poison .....	98
Triggered updates .....	98
Multicast .....	98
Default.....	98
Metric.....	98
Authentication .....	98
RIP configuration example .....	99
<b>IGMP Snooping</b>	
Introduction .....	100
Overview .....	100
FastLeave .....	100
IGMP Filtering .....	101
Static multicast router.....	101
IGMP Snooping configuration example.....	101

## OSPF

OSPF overview .....	111
Types of OSPF areas .....	111
Types of OSPF routing devices .....	112
Neighbors and adjacencies .....	113
Link-State Database .....	113
Shortest Path First Tree .....	113
Internal versus external routing .....	113
OSPF implementation in GbE2 software .....	114
Configurable parameters .....	114
Defining areas .....	114
Interface cost .....	116
Electing the designated router and backup .....	116
Summarizing routes .....	116
Default routes .....	117
Virtual links .....	117
Router ID .....	118
Authentication .....	118
Host routes for load balancing .....	119
OSPF features not supported in this release .....	120
OSPF configuration examples .....	120
Example 1: Simple OSPF domain (CLI example) .....	120
Example 2: Virtual links .....	128
Configuring OSPF for a virtual link on Switch B .....	130
Example 3: Summarizing routes .....	131
Verifying OSPF configuration .....	132

## Remote monitoring

Introduction .....	133
Overview .....	133
RMON group 1—statistics .....	133
RMON group 2—history .....	136
RMON group 3—alarms .....	137
RMON group 9—events .....	141

## High availability

Introduction .....	143
Uplink Failure Detection .....	143
Failure Detection Pair .....	144
Spanning Tree Protocol with UFD .....	144
Configuration guidelines .....	144
Monitoring Uplink Failure Detection .....	144
Configuring Uplink Failure Detection .....	145
VRRP overview .....	148
VRRP components .....	148
VRRP operation .....	149
Selecting the master VRRP router .....	149
Failover methods .....	149
Active-Active redundancy .....	150
GbE2 extensions to VRRP .....	150
Tracking VRRP router priority .....	150
Virtual router deployment considerations .....	151
Assigning VRRP virtual router ID .....	151
Configuring the switch for tracking .....	151
High availability configurations .....	151
Active-Active configuration .....	152

## Troubleshooting tools

Introduction .....	163
Port Mirroring .....	163
Configuring Port Mirroring (CLI example) .....	164
Configuring Port Mirroring (BBI example) .....	165
Other network troubleshooting techniques .....	167
Console and Syslog messages .....	167
Ping .....	167
Trace route .....	167
Statistics and state information .....	167
Customer support tools .....	167

## Index

# Accessing the GbE2 Interconnect Switch

## Introduction

This guide will help you plan, implement, and administer the HP ProLiant BL p-Class GbE2 Interconnect Switch software. Where possible, each section provides feature overviews, usage examples, and configuration instructions.

- **"Accessing the GbE2 Interconnect Switch"** describes how to configure and view information and statistics on the GbE2 Interconnect Switch over an IP network. This chapter also discusses different methods to manage the GbE2 Interconnect Switch for remote administrators, such as setting specific IP addresses and using Remote Authentication Dial-in User Service (RADIUS) authentication, Secure Shell (SSH), and Secure Copy (SCP) for secure access to the switch.
- **"Ports and Port Trunking"** describes how to group multiple physical ports together to aggregate the bandwidth between large-scale network devices.
- **"Port-based Network Access and Traffic Control"** describes how to authenticate devices attached to a LAN port that has point-to-point connection characteristics. Port-based Network Access Control provides security to ports of the GbE2 that connect to servers. Port-based Traffic Control allows the switch to guard against broadcast storms.
- **"VLANs"** describes how to configure Virtual Local Area Networks (VLANs) for creating separate network segments, including how to use VLAN tagging for devices that use multiple VLANs.
- **"Spanning Tree Protocol"** discusses how spanning trees configure the network so that the GbE2 Interconnect Switch uses the most efficient path when multiple paths exist.
- **"Rapid Spanning Tree Protocol/Multiple Spanning Tree Protocol"** describes extensions to the Spanning Tree Protocol that provide rapid convergence of spanning trees for fast reconfiguration of the network.
- **"Quality of Service"** discusses Quality of Service features, including IP filtering using Access Control Lists, Differentiated Services, and IEEE 802.1p priority values.
- **"Basic IP Routing"** describes how to configure the GbE2 Interconnect Switch for IP routing using IP subnets, and DHCP Relay.
- **"Routing Information Protocol"** describes how the GbE2 software implements standard RIP for exchanging TCP/IP route information with other routers.
- **"IGMP Snooping"** describes how to use IGMP to conserve bandwidth in a multicast-switching environment.
- **"OSPF"** describes OSPF concepts, how OSPF is implemented, and examples of how to configure your switch for OSPF support.
- **"Remote Monitoring"** describes how to configure the RMON agent on the GbE2 Interconnect Switch, so the switch can exchange network monitoring data.
- **"High Availability"** describes how the GbE2 Interconnect Switch supports high-availability network topologies. This release provides Uplink Failure Detection and Virtual Router Redundancy Protocol.
- **"Troubleshooting Tools"** describes Port Mirroring and other troubleshooting techniques.

## Additional references

Additional information about installing and configuring the GbE2 Interconnect Switch is available in the following guides, which are available at <http://www.hp.com>.

- *HP ProLiant BL p-Class GbE2 Interconnect Switch User Guide*
- *HP ProLiant BL p-Class GbE2 Interconnect Switch Command Reference Guide*
- *HP ProLiant BL p-Class GbE2 Interconnect Switch ISCLI Reference Guide*
- *HP ProLiant BL p-Class GbE2 Interconnect Switch Browser-based Interface Reference Guide*
- *HP ProLiant BL p-Class C-GbE2 Interconnect Kit Quick Setup Instructions*
- *HP ProLiant BL p-Class F-GbE2 Interconnect Kit Quick Setup Instructions*
- *HP BladeSystem p-Class SAN Connectivity Kit Quick Setup Instructions*

# Typographical conventions

The following table describes the typographic styles used in this guide:

**Table 1** Typographic conventions

Typeface or symbol	Meaning	Example
AaBbCc123	This type depicts onscreen computer output and prompts.	Main#
AaBbCc123	This type displays in command examples and shows text that must be typed in exactly as shown.	Main# sys
<AaBbCc123>	This italicized type displays in command examples as a parameter placeholder. Replace the indicated text with the appropriate real name or value when using the command. Do not type the brackets. This also shows guide titles, special terms, or words to be emphasized.	To establish a Telnet session, enter: host# telnet <IP address> Read your user guide thoroughly.
[ ]	Command items shown inside brackets are optional and can be used or excluded as the situation demands. Do not type the brackets.	host# ls [-a]

## Using the command line interface

The command line interface (CLI) can be accessed via local terminal connection or a remote session using Telnet or SSH. The CLI is the most direct method for collecting GbE2 Interconnect Switch information and performing switch configuration. The Main Menu of the CLI with administrator privileges is displayed in the following table:

[Main Menu]	<ul style="list-style-type: none"><li>info - Information Menu</li><li>stats - Statistics Menu</li><li>cfg - Configuration Menu</li><li>oper - Operations Command Menu</li><li>boot - Boot Options Menu</li><li>maint - Maintenance Menu</li><li>diff - Show pending config changes [global command]</li><li>apply - Apply pending config changes [global command]</li><li>save - Save updated config to FLASH [global command]</li><li>revert - Revert pending or applied changes [global command]</li><li>exit - Exit [global command, always available]</li></ul>
-------------	---

## Connecting through the console port

Using a null modem cable, you can directly connect to the GbE2 Interconnect Switch through the console port. A console connection is required in order to configure Telnet or other remote access applications. For more information on establishing console connectivity to the GbE2 Interconnect Switch, see the *HP ProLiant BL p-Class GbE2 Interconnect Switch User Guide*.

## Configuring an IP interface

An IP interface address must be set on the GbE2 Interconnect Switch to provide management access to the switch over an IP network. By default, the management interface is set up to request its IP address from a Bootstrap Protocol (BOOTP) server.

If you have a BOOTP server on your network, add the Media Access Control (MAC) address of the GbE2 Interconnect Switch to the BOOTP configuration file located on the BOOTP server. The MAC address can be found on a small white label on the back panel of the GbE2 Interconnect Switch. The MAC address can also be found in the System Information menu (See the "System information" section in the "Information Menu" chapter of the *HP ProLiant BL p-Class GbE2 Interconnect Switch Command Reference Guide*.) If you are using a DHCP server that also does BOOTP, you do not have to configure the MAC address.

If you do not have a BOOTP server, you must manually configure an IP address.

The following example shows how to manually configure an IP address on the GbE2 Interconnect Switch:

1. Configure an IP interface for the Telnet connection, using the sample IP address of 205.21.17.3.
2. The pending subnet mask address and broadcast address are automatically calculated.

```
>> # /cfg/13/if 1                                (Select IP interface 1)
>> IP Interface 1# addr 205.21.17.3   (Assign IP address for the interface)
Current IP address:      0.0.0.0
New pending IP address: 205.21.17.3
Pending new subnet mask:    255.255.255.0
. . . . .
>> IP Interface 1# ena                           (Enable IP interface 1)
```

3. If necessary, configure up to four default gateways.
4. Configuring the default gateways allows the GbE2 Interconnect Switch to send outbound traffic to the routers.

```
>> IP Interface 5# ../gw 1                      (Select primary default gateway)
>> Default gateway 1# addr 205.21.17.1       (Assign IP address for primary router)
>> Default gateway 1# ena                     (Enable primary default gateway)
>> Default gateway 1# ../gw 2                  (Select secondary default gateway)
>> Default gateway 2# addr 205.21.17.2       (Assign address for secondary router)
>> Default gateway 2# ena                     (Enable secondary default gateway)
```

5. Apply, verify, and save the configuration.

```
>> Default gateway 2# apply                   (Apply the configuration)
>> Default gateway 2# save                   (Save the configuration)
>> # /cfg/dump                            (Verify the configuration)
```

## Connecting via Telnet

By default, Telnet is enabled on the GbE2 Interconnect Switch. Once the IP parameters are configured, you can access the CLI from any workstation connected to the network using a Telnet connection. Telnet access provides the same options for a user and an administrator as those available through the console port, minus certain commands. The GbE2 Interconnect Switch supports four concurrent Telnet connections.

To establish a Telnet connection with the GbE2 Interconnect Switch, run the Telnet program on your workstation and issue the **telnet** command, followed by the switch IP address:

```
telnet <switch IP address>
```

## Connecting via Secure Shell

By default, the Secure Shell (SSH) protocol is disabled on the GbE2 Interconnect Switch. SSH enables you to securely log into another computer over a network to execute commands remotely. As a secure alternative to using Telnet to manage switch configuration, SSH ensures that all data sent over the network is encrypted and secure. For more information, see the "Secure Shell and Secure Copy" section later in this chapter. For additional information on the CLI, refer to the *HP ProLiant BL p-Class GbE2 Interconnect Switch Command Reference Guide*.

## Using the Browser-based Interface

By default, the Browser-based Interface (BBI) protocol is enabled on the GbE2 Interconnect Switch. The Browser-based Interface (BBI) provides access to the common configuration, management and operation features of the switch through your Web browser. For more information, see the *HP ProLiant BL p-Class GbE2 Interconnect Switch BBI Reference Guide*.

The BBI is organized at a high level as follows:

- **Configuration**—These menus provide access to the configuration elements for the entire switch.
  - **System**—Configure general switch configuration elements.
  - **Switch Ports**—configure switch ports and related features.
  - **Port-Based Port Mirroring**—Configure mirrored ports and monitoring ports.
  - **Layer 2**—Configure Layer 2 features, including Trunk Groups, VLANs, and Spanning Tree Protocol.
  - **RMON Menu**—Configure Remote Monitoring (RMON) functions.
  - **Layer 3**—Configure all of the IP related information, including IGMP Snooping, OSPF, and Virtual Router Redundancy Protocol (VRRP).
  - **QoS**—Configure Quality of Service features.
  - **Access Control**—Configure Access Control Lists, Blocks, and Groups.
  - **Uplink Failure Detection**—Configure a Failover Pair of Links to Monitor and Links to Disable.
- **Statistics**—These menus provide access to the switch statistics and state information.
- **Dashboard**—These menus display settings and operating status of a variety of switch features.

## Using Simple Network Management Protocol

GbE2 software provides SNMP v1.0 and SNMP v3.0 support for access through any network management software, such as HP-OpenView.

### SNMP v1.0

To access the SNMP agent on the GbE2, the read and write community strings on the SNMP manager should be configured to match those on the switch. The default read community string on the switch is **public** and the default write community string is **private**.

The read and write community strings on the switch can be changed using the following commands on the CLI.

```
>> /cfg/sys/ssnmp/rcomm
```

and

```
>> /cfg/sys/ssnmp/wcomm
```

The SNMP manager should be able to reach the management interface or any one of the IP interfaces on the switch.

For the SNMP manager to receive the traps sent out by the SNMP agent on the switch, the trap host on the switch should be configured with the following command:

```
/cfg/sys/ssnmp/snmpv3/taddr
```

For more details, see “Configuring SNMP Trap Hosts”.

### SNMP v3.0

SNMPv3 is an enhanced version of the Simple Network Management Protocol, approved by the Internet Engineering Steering Group in March, 2002. SNMP v3.0 contains additional security and authentication features that provide data origin authentication, data integrity checks, timeliness indicators and encryption to protect against threats such as masquerade, modification of information, message stream modification and disclosure.

SNMP v3 ensures that the client can use SNMP v3 to query the MIBs, mainly for security.

To access the SNMP v3.0 menu, enter the following command in the CLI:

```
>> # /cfg/sys/ssnmp/snmpv3
```

For more information on SNMP MIBs and the commands used to configure SNMP on the switch, see the *HP ProLiant BL p-Class GbE2 Interconnect Switch Command Reference Guide*.

## Default configuration

GbE2 software has two users by default. Both the users 'adminmd5' and 'adminsha' have access to all the MIBs supported by the switch.

1. username 1: adminmd5/password adminmd5. Authentication used is MD5.
2. username 2 adminsha/password adminsha. Authentication used is SHA.
3. username 3 v1v2only/password none.

To configure an SNMP user name, enter the following command from the CLI:

```
>> # /cfg/sys/ssnmp/snmpv3/usm <username>
```

## User configuration

Users can be configured to use the authentication/privacy options. Currently we support two authentication algorithms: MD5 and SHA. These can be specified using the command:

```
/cfg/sys/ssnmp/snmpv3/usm <x>/auth md5 | sha
```

1. To configure a user with name 'test,' authentication type MD5, and authentication password of 'test,' privacy option DES with privacy password of 'test,' use the following CLI commands

```
>> # /cfg/sys/ssnmp/snmpv3/usm 5
>> SNMPv3 usmUser 5 # name "test"
>> SNMPv3 usmUser 5 # auth md5
>> SNMPv3 usmUser 5 # authpw test
>> SNMPv3 usmUser 5 # priv des
>> SNMPv3 usmUser 5 # privpw test
```

2. Once a user is configured you need to specify the access level for this user along with the views the user is allowed access to. This is specified in the access table.

```
>> # /cfg/sys/ssnmp/snmpv3/access 5
>> SNMPv3 vacmAccess 5 # name "testgrp"
>> SNMPv3 vacmAccess 5 # level authPriv
>> SNMPv3 vacmAccess 5 # rview "iso"
>> SNMPv3 vacmAccess 5 # wview "iso"
>> SNMPv3 vacmAccess 5 # nview "iso"
```

3. The group table links the user to a particular access group.

```
>> # /cfg/sys/ssnmp/snmpv3/group 5
>> SNMPv3 vacmSecurityToGroup 5 # uname test
>> SNMPv3 vacmSecurityToGroup 5 # gname testgrp
```

If you want to allow user access only to certain MIBs, see the "View based Configuration" section.

## View based configurations

### CLI user equivalent

To configure an SNMP user equivalent to the CLI 'user,' use the following configuration:

```
/c/sys/ssnmp/snmpv3/usm 4
name "usr"
/c/sys/ssnmp/snmpv3/access 3
name "usrgrp"
rview "usr"
wview "usr"
nview "usr"
/c/sys/ssnmp/snmpv3/group 4
uname usr
gname usrrgp
/c/sys/ssnmp/snmpv3/view 6
name "usr"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.1.2"
/c/sys/ssnmp/snmpv3/view 7
name "usr"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.1.3"
/c/sys/ssnmp/snmpv3/view 8
name "usr"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.2.2"
/c/sys/ssnmp/snmpv3/view 9
name "usr"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.2.3"
/c/sys/ssnmp/snmpv3/view 10
name "usr"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.3.2"
/c/sys/ssnmp/snmpv3/view 11
name "usr"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.3.3"
```

### CLI oper equivalent

To configure an SNMP user equivalent to the CLI 'oper,' use the following configuration:

```
/c/sys/ssnmp/snmpv3/usm 5
name "oper"
/c/sys/ssnmp/snmpv3/access 4
name "opergrp"
rview "oper"
wview "oper"
nview "oper"
/c/sys/ssnmp/snmpv3/group 4
uname oper
gname opergrp
/c/sys/ssnmp/snmpv3/view 20
name "oper"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.1.2"
/c/sys/ssnmp/snmpv3/view 21
name "oper"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.1.3"
/c/sys/ssnmp/snmpv3/view 22
name "oper"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.2.2"
/c/sys/ssnmp/snmpv3/view 23
name "oper"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.2.3"
/c/sys/ssnmp/snmpv3/view 24
name "oper"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.3.2"
/c/sys/ssnmp/snmpv3/view 25
name "oper"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.3.3"
```

## Configuring SNMP trap hosts

### SNMPv1 trap host

1. Configure a user with no authentication and password.

```
/c/sys/ssnmp/snmpv3/usm 10  
name "vltrap"
```

2. Configure an access group and group table entries for the user. The command

/c/sys/ssnmp/snmpv3/access <x>/nview can be used to specify which traps can be received by the user. In the example below the user will receive the traps sent by the switch.

```
/c/sys/ssnmp/snmpv3/access 10  
name "vltrap"  
model snmpv1  
nview "iso"  
/c/sys/ssnmp/snmpv3/group 10  
model snmpv1  
uname vltrap  
gname vltrap
```

3. Configure an entry in the notify table.

```
/c/sys/ssnmp/snmpv3/notify 10  
name vltrap  
tag vltrap
```

4. Specify the IP address and other trap parameters in the targetAddr and targetParam tables. The c/sys/ssnmp/snmpv3/tparam <x>/uname command is used to specify the user name used with this targetParam table.

```
/c/sys/ssnmp/snmpv3/taddr 10  
name vltrap  
addr 47.80.23.245  
taglist vltrap  
pname v1param  
/c/sys/ssnmp/snmpv3/tparam 10  
name v1param  
mpmodel snmpv1  
uname vltrap  
model snmpv1
```

5. The community string used in the traps is specified using the community table.

```
/c/sys/ssnmp/snmpv3/comm 10  
index vltrap  
name public  
uname vltrap
```

## SNMPv2 trap host configuration

The SNMPv2 trap host configuration is similar to the SNMPv1 trap host configuration. Wherever you specify the model you need to specify snmpv2 instead of snmpv1.

```
c/sys/ssnmp/snmpv3/usm 10
  name "v2trap"
/c/sys/ssnmp/snmpv3/access 10
  name "v2trap"
  model snmpv2
  nview "iso"
/c/sys/ssnmp/snmpv3/group 10
  model snmpv2
  uname v2trap
  gname v2trap
/c/sys/ssnmp/snmpv3/taddr 10
  name v2trap
  addr 47.81.25.66
  taglist v2trap
  pname v2param
/c/sys/ssnmp/snmpv3/tparam 10
  name v2param
  mpmodel snmpv2c
  uname v2trap
  model snmpv2
/c/sys/ssnmp/snmpv3/notify 10
  name v2trap
  tag v2trap
/c/sys/ssnmp/snmpv3/comm 10
  index v2trap
  name public
  uname v2trap
```

## SNMPv3 trap host configuration

To configure a user for SNMPv3 traps you can choose to send the traps with both privacy and authentication, with authentication only, or without privacy or authentication.

This is configured in the access table using the command: /c/sys/ssnmp/snmpv3/access <x>/level, and /c/sys/ssnmp/snmpv3/tparam <x>. The user in the user table should be configured accordingly.

It is not necessary to configure the community table for SNMPv3 traps because the community string is not used by SNMPv3.

The following example shows how to configure a SNMPv3 user v3trap with authentication only:

```
/c/sys/ssnmp/snmpv3/usm 11
  name "v3trap"
  auth md5
  authpw v3trap
/c/sys/ssnmp/snmpv3/access 11
  name "v3trap"
  level authNoPriv
  nview "iso"
/c/sys/ssnmp/snmpv3/group 11
  uname v3trap
  gname v3trap
/c/sys/ssnmp/snmpv3/taddr 11
  name v3trap
  addr 47.81.25.66
  taglist v3trap
  pname v3param
/c/sys/ssnmp/snmpv3/tparam 11
  name v3param
  uname v3trap
  level authNoPriv
/c/sys/ssnmp/snmpv3/notify 11
  name v3trap
  tag v3trap
```

For more information on using SNMP, see the *HP ProLiant BL p-Class GbE2 Interconnect Switch Command Reference Guide*.

Refer to the HP ProLiant BL p-Class GbE2 Interconnect Switch Management Utilities for a complete list of supported MIBs. The utilities package is located at the following website: <http://www.hp.com/support>.

## Secure access to the switch

Secure switch management is needed for environments that perform significant management functions across the Internet. The following are some of the functions for secured management:

- Limiting management users to a specific IP address range. See the “Setting allowable source IP address ranges” section in this chapter.
- Authentication and authorization of remote administrators. See the “RADIUS authentication and authorization” section or the “TACACS+ authentication” section, both later in this chapter.
- Encryption of management information exchanged between the remote administrator and the switch. See the “Secure Shell and Secure Copy” section later in this chapter.

### Setting allowable source IP address ranges

To limit access to the GbE2 Interconnect Switch without having to configure filters for each switch port, you can set a source IP address (or range) that will be allowed to connect to the GbE2 Interconnect Switch IP interface through Telnet, SSH, SNMP, or the GbE2 Interconnect Switch browser-based interface (BBI).

When an IP packet reaches the application switch, the source IP address is checked against the range of addresses defined by the management network and mask (**mnet** and **mmask**). If the source IP address of the host or hosts is within this range, it is allowed to attempt to log in. Any packet addressed to a GbE2 Interconnect Switch IP interface with a source IP address outside this range is discarded.

### Configuring an IP address range for the management network

Configure the management network IP address and mask from the System Menu in the CLI. For example:

```
>> Main# /cfg/sys/access/mgmt/add  
Enter Management Network Address: 192.192.192.0  
Enter Management Network Mask: 255.255.255.128
```

In this example, the management network is set to 192.192.192.0 and management mask is set to 255.255.255.128. This defines the following range of allowed IP addresses: 192.192.192.1 to 192.192.192.127.

The following source IP addresses are granted or not granted access to the GbE2 Interconnect Switch:

- A host with a source IP address of 192.192.192.21 falls within the defined range and would be allowed to access the GbE2 Interconnect Switch.
- A host with a source IP address of 192.192.192.192 falls outside the defined range and is not granted access. To make this source IP address valid, you would need to shift the host to an IP address within the valid range specified by the **mnet** and **mmask** or modify the **mnet** to be 192.192.192.128 and the **mmask** to be 255.255.255.128. This would put the 192.192.192.192 host within the valid range allowed by the **mnet** and **mmask** (192.192.192.128-255).

### RADIUS authentication and authorization

The GbE2 Interconnect Switch supports the Remote Authentication Dial-in User Service (RADIUS) method to authenticate and authorize remote administrators for managing the GbE2 Interconnect Switch. This method is based on a client/server model. The Remote Access Server (RAS)—the switch—is a client to the back-end database server. A remote user (the remote administrator) interacts only with the RAS, not the back-end server and database.

RADIUS authentication consists of the following components:

- A protocol with a frame format that utilizes User Datagram Protocol (UDP) over IP, based on Request For Comments (RFC) 2138 and 2866
- A centralized server that stores all the user authorization information
- A client, in this case, the GbE2 Interconnect Switch

The GbE2 Interconnect Switch, acting as the RADIUS client, communicates to the RADIUS server to authenticate and authorize a remote administrator using the protocol definitions specified in RFC 2138 and 2866. Transactions between the client and the RADIUS server are authenticated using a shared key that is not sent over the network. In addition, the remote administrator passwords are sent encrypted between the RADIUS client (the switch) and the back-end RADIUS server.

## How RADIUS authentication works

RADIUS authentication works as follows:

1. A remote administrator connects to the GbE2 Interconnect Switch and provides the user name and password.
2. Using Authentication/Authorization protocol, the GbE2 Interconnect Switch sends the request to the authentication server.
3. The authentication server checks the request against the user ID database.
4. Using RADIUS protocol, the authentication server instructs the GbE2 Interconnect Switch to grant or deny administrative access.

## Configuring RADIUS on the switch (CLI example)

To configure RADIUS on the GbE2 Interconnect Switch, do the following:

1. Turn RADIUS authentication on, and then configure the Primary and Secondary RADIUS servers. For example:

```
>> Main# /cfg/sys/radius          (Select the RADIUS Server menu)
>> RADIUS Server# on             (Turn RADIUS on)
Current status: OFF
New status:      ON
>> RADIUS Server# prisrv 10.10.1.1    (Enter primary server IP)
Current primary RADIUS server:   0.0.0.0
New pending primary RADIUS server: 10.10.1.1
>> RADIUS Server# secsrv 10.10.1.2    (Enter secondary server IP)
Current secondary RADIUS server:  0.0.0.0
New pending secondary RADIUS server: 10.10.1.2
```

2. Configure the primary RADIUS secret and secondary RADIUS secret.

```
>> RADIUS Server# secret
Enter new RADIUS secret: <1-32 character secret>
>> RADIUS Server# secret2
Enter new RADIUS second secret: <1-32 character secret>
```



**CAUTION:** If you configure the RADIUS secret using any method other than a direct console connection, the secret may be transmitted over the network as clear text.

3. If desired, you may change the default User Datagram Protocol (UDP) port number used to listen to RADIUS. The well-known port for RADIUS is 1645.

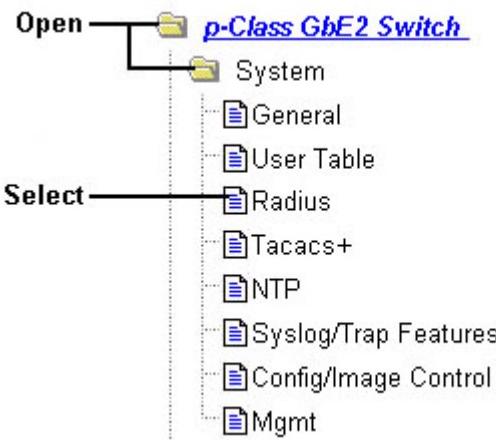
```
>> RADIUS Server# port
Current RADIUS port: 1645
Enter new RADIUS port [1500-3000]: <port number>
```

4. Configure the number of retry attempts for contacting the RADIUS server, and the timeout period.

```
>> RADIUS Server# retries  
Current RADIUS server retries: 3  
Enter new RADIUS server retries [1-3]:<server retries>  
>> RADIUS Server# time  
Current RADIUS server timeout: 3  
Enter new RADIUS server timeout [1-10]: 10 (Enter the timeout period  
in seconds)
```

## Configuring RADIUS on the switch (BBI example)

1. Configure RADIUS parameters.
  - a. Click the **Configure** context button.
  - b. Open the System folder, and select **Radius**.

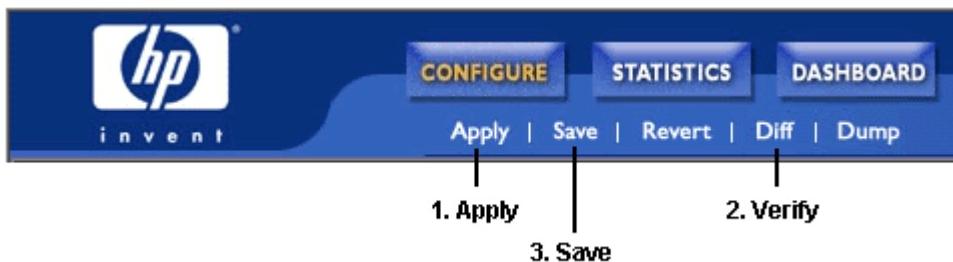


- c. Enter the IP address of the primary and secondary RADIUS servers, and enter the RADIUS secret for each server. Enable the RADIUS server.

Switch Radius Configuration	
Primary Radius IP Address	10.10.1.1
Secondary Radius IP Address	10.10.1.2
Radius port (1500-3000)	1645
Radius timeout (1-10)	3
Radius retries (1-3)	3
Enable/Disable Radius Server	Enabled
Enable/Disable Radius Backdoor for telnet	Disabled
Enable/Disable Radius Secure Backdoor for telnet	Disabled
Radius Secret	secret_one
Secondary Radius Server Secret	secret_two
<b>Submit</b>	

**CAUTION:** If you configure the RADIUS secret using any method other than a direct console connection, the secret may be transmitted over the network as clear text.

- d. Click **Submit**.  
 2. Apply, verify, and save the configuration.



## RADIUS authentication features

The GbE2 Interconnect Switch supports the following RADIUS authentication features:

- Supports RADIUS client on the GbE2 Interconnect Switch, based on the protocol definitions in RFC 2138 and RFC 2866.
- Allows RADIUS secret password up to 32 bytes.
- Supports secondary authentication server so that when the primary authentication server is unreachable, the GbE2 Interconnect Switch can send client authentication requests to the secondary authentication server. Use the `/cfg/sys/radius/cur` command to show the currently active RADIUS authentication server.
- Supports user-configurable RADIUS server retry and time-out values:
  - Time-out value = 1-10 seconds
  - Retries = 1-3
- The GbE2 Interconnect Switch will time out if it does not receive a response from the RADIUS server in one to three retries. The GbE2 Interconnect Switch will also automatically retry connecting to the RADIUS server before it declares the server down.
- Supports user-configurable RADIUS application port. The default is 1645/User Datagram Protocol (UDP)-based on RFC 2138. Port 1812 is also supported.

- Allows network administrator to define privileges for one or more specific users to access the GbE2 Interconnect Switch at the RADIUS user database.
- Allows the administrator to configure RADIUS backdoor and secure backdoor for Telnet, SSH, HTTP, and HTTPS access.

## User accounts for RADIUS users

The user accounts listed in the following table can be defined in the RADIUS server dictionary file.

**Table 2** User access levels

User account	Description and tasks performed
User	User interaction with the GbE2 Interconnect Switch is completely passive; nothing can be changed on the GbE2 Interconnect Switch. Users may display information that has no security or privacy implications, such as GbE2 Interconnect Switch statistics and current operational state information.
Operator	Operators can only effect temporary changes on the GbE2 Interconnect Switch. These changes are lost when the GbE2 Interconnect Switch is rebooted/reset. Operators have access to the GbE2 Interconnect Switch management features used for daily switch operations. Because any changes an operator makes are undone by a reset of the GbE2 Interconnect Switch, operators cannot severely impact switch operation, but do have access to the Maintenance menu. By default, the operator account is disabled and has no password.
Administrator	Administrators are the only ones that can make permanent changes to the switch configuration—changes that are persistent across a reboot/reset of the GbE2 Interconnect Switch. Administrators can access GbE2 Interconnect Switch functions to configure and troubleshoot problems on the switch level. Because administrators can also make temporary (operator-level) changes as well, they must be aware of the interactions between temporary and permanent changes.

## RADIUS attributes for user privileges

When the user logs in, the GbE2 Interconnect Switch authenticates the level of access by sending the RADIUS access request, that is, the client authentication request, to the RADIUS authentication server.

If the authentication server successfully authenticates the remote user, the GbE2 Interconnect Switch verifies the privileges of the remote user and authorizes the appropriate access. The administrator has the option to allow backdoor access through the console port only, or through the console and Telnet/SSH/HTTP/HTTPS access. When backdoor access is enabled, access is allowed even if the primary and secondary authentication servers are not reachable. Only when both the primary and secondary authentication servers are not reachable, the administrator has the option to allow secure backdoor (secbdr) access through the console port only, or through the console and Telnet/SSH/HTTP/HTTPS access. When RADIUS is on, you can have either backdoor or secure backdoor allowed, not both. The default value for backdoor access through the console port only is enabled. The default value for backdoor and secure backdoor access through Telnet/SSH/HTTP/HTTPS is disabled.

All user privileges, other than those assigned to the administrator, must be defined in the RADIUS dictionary. RADIUS attribute 6, which is built into all RADIUS servers, defines the administrator. The file name of the dictionary is RADIUS vendor-dependent. The RADIUS attributes shown in the following table are defined for user privilege levels.

**Table 3** Proprietary attributes for RADIUS

User name/access	User service type	Value
User	Vendor-supplied	255
Operator	Vendor-supplied	252

## TACACS+ authentication

GbE2 software supports authentication, authorization, and accounting with networks using the Cisco Systems TACACS+ protocol. The HP ProLiant BL p-Class GbE2 Interconnect Switch functions as the Network Access Server (NAS) by interacting with the remote client and initiating authentication and authorization sessions with the TACACS+ access server. The remote user is defined as someone requiring management access to the HP ProLiant BL p-Class GbE2 Interconnect Switch either through a data or management port.

TACACS+ offers the following advantages over RADIUS:

- TACACS+ uses TCP-based connection-oriented transport; whereas RADIUS is UDP based. TCP offers a connection-oriented transport, while UDP offers best-effort delivery. RADIUS requires additional programmable variables such as re-transmit attempts and time-outs to compensate for best-effort transport, but it lacks the level of built-in support that a TCP transport offers.
- TACACS+ offers full packet encryption whereas RADIUS offers password-only encryption in authentication requests.
- TACACS+ separates authentication, authorization, and accounting.

## How TACACS+ authentication works

TACACS+ works much in the same way as RADIUS authentication.

1. Remote administrator connects to the switch and provides user name and password.

 **NOTE:** The user name and password can have a maximum length of 15 characters. The password cannot be left blank.

2. Using Authentication/Authorization protocol, the switch sends request to authentication server.
3. Authentication server checks the request against the user ID database.
4. Using TACACS+ protocol, the authentication server instructs the switch to grant or deny administrative access.

During a session, if additional authorization checking is needed, the switch checks with a TACACS+ server to determine if the user is granted permission to use a particular command.

## TACACS+ authentication features in GbE2 Interconnect Switch

Authentication is the action of determining the identity of a user, and is generally done when the user first attempts to log in to a device or gain access to its services. GbE2 software supports ASCII inbound login to the device. PAP, CHAP and ARAP login methods, TACACS+ change password requests, and one-time password authentication are not supported.

## Authorization

Authorization is the action of determining a user's privileges on the device, and usually takes place after authentication.

The default mapping between TACACS+ authorization privilege levels and switch management access levels is shown in the table below. The privilege levels listed in the following table must be defined on the TACACS+ server.

**Table 4** Default TACACS+ privilege levels

User access level	TACACS+ level
user	0
oper	3
admin	6

Alternate mapping between TACACS+ privilege levels and GbE2 management access levels is shown in the table below. Use the command /cfg/sys/tacacs/cmap ena to use the alternate TACACS+ privilege levels.

**Table 5** Alternate TACACS+ privilege levels

User access level	TACACS+ level
user	0 - 1
oper	6 - 8
admin	14 - 15

You can customize the mapping between TACACS+ privilege levels and GbE2 management access levels. Use the /cfg/sys/tacacs/usermap command to manually map each TACACS+ privilege level (0-15) to a corresponding GbE2 management access level (user, oper, admin, none).

If the remote user is authenticated by the authentication server, the GbE2 verifies the **privileges** of the remote user and authorizes the appropriate access. When both the primary and secondary authentication servers are not reachable, the administrator has an option to allow **backdoor** access via the console only or console and Telnet access. The default is **disable** for Telnet access and **enable** for console access. The administrator also can enable **secure backdoor** (/cfg/sys/tacacs/secb) to allow access if both the primary and secondary TACACS+ servers fail to respond.

## Accounting

Accounting is the action of recording a user's activities on the device for the purposes of billing and/or security. It follows the authentication and authorization actions. If the authentication and authorization is not performed via TACACS+, no TACACS+ accounting messages are sent out.

You can use TACACS+ to record and track software logins, configuration changes, and interactive commands.

The switch supports the following TACACS+ accounting attributes:

- protocol (console/telnet/ssh/http)
- start\_time
- stop\_time
- elapsed\_time

 **NOTE:** When using the Browser-based Interface, the TACACS+ Accounting **Stop** records are sent only if the **Quit** button on the browser is clicked.

## Configuring TACACS+ authentication on the switch (CLI example)

1. Turn TACACS+ authentication on, then configure the Primary and Secondary TACACS+ servers.

```
>> Main# /cfg/sys/tacacs          (Select the TACACS+ Server menu)
>> TACACS+ Server# on           (Turn TACACS+ on)
Current status: OFF
New status: ON
>> TACACS+ Server# prisrv 10.10.1.1 (Enter primary server IP)
Current primary TACACS+ server: 0.0.0.0
New pending primary TACACS+ server: 10.10.1.1
>> TACACS+ Server# secsrv 10.10.1.2 (Enter secondary server IP)
Current secondary TACACS+ server: 0.0.0.0
New pending secondary TACACS+ server: 10.10.1.2
```

- Configure the TACACS+ secret and second secret.

```
>> TACACS+ Server# secret  
  
Enter new TACACS+ secret: <1-32 character secret>  
>> TACACS+ Server# secret2  
Enter new TACACS+ second secret: <1-32 character secret>
```



**CAUTION:** If you configure the TACACS+ secret using any method other than a direct console connection, the secret may be transmitted over the network as clear text.

- If desired, you may change the default TCP port number used to listen to TACACS+.
- The well-known port for TACACS+ is 49.

```
>> TACACS+ Server# port  
Current TACACS+ port: 49  
Enter new TACACS+ port [1-65000]: <port number>
```

- Configure the number retry attempts for contacting the TACACS+ server and the timeout period.

```
>> TACACS+ Server# retries  
Current TACACS+ server retries: 3  
Enter new TACACS+ server retries [1-3]: 2  
>> TACACS+ Server# time  
Current TACACS+ server timeout: 5  
Enter new TACACS+ server timeout [4-15]: 10 (Enter the timeout period  
in minutes)
```

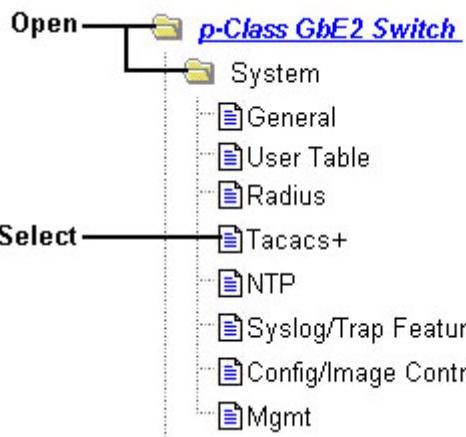
- Configure custom privilege-level mapping (optional).

```
>> TACACS+ Server# usermap 2  
Current privilege mapping for remote privilege 2: not set  
Enter new local privilege mapping: user  
>> TACACS+ Server# usermap 3 user  
>> TACACS+ Server# usermap 4 user  
>> TACACS+ Server# usermap 5 oper
```

- Apply and save the configuration.

## Configuring TACACS+ authentication on the switch (BBI example)

1. Configure TACACS+ authentication for the switch.
  - a. Click the **Configure** context button.
  - b. Open the System folder, and select **Tacacs+**.



- c. Enter the IP address of the primary and secondary TACACS+ servers, and enter the TACACS+ secret. Enable TACACS+.

**Switch Tacacs+ Configuration**

Primary Tacacs+ IP Address	10.10.1.1
Secondary Tacacs+ IP Address	10.10.1.2
Tacacs+ port (1-65000)	49
Tacacs+ timeout (4-15)	5
Tacacs+ retries (1-3)	3
Enable/Disable Tacacs+ Server	Enabled
Enable/Disable Tacacs+ Backdoor for telnet	Disabled
Enable/Disable Tacacs+ Secure Backdoor for telnet	Disabled
Enable/Disable Tacacs+ new privilege level mapping	Disabled
Tacacs+ Secret	
Secondary Tacacs+ Server Secret	

- d. Click **Submit**.

- e. Configure custom privilege-level mapping (optional). Click **Submit** to accept each mapping change.

Remote privilege	Local privilege
5	<input style="width: 60px; height: 25px; border: 1px solid black; padding: 2px; margin-bottom: 5px;" type="button" value="Oper"/> ▼
0	not set
1	user
2	user
3	user
4	user
5	not set
⋮	
14	not set
15	not set

2. Apply, verify, and save the configuration.



## Secure Shell and Secure Copy

Secure Shell (SSH) and Secure Copy (SCP) use secure tunnels to encrypt and secure messages between a remote administrator and the GbE2 Interconnect Switch. Telnet does not provide this level of security. The Telnet method of managing a GbE2 Interconnect Switch does not provide a secure connection.

SSH is a protocol that enables remote administrators to log securely into the GbE2 Interconnect Switch over a network to execute management commands. By default, SSH is disabled (off) on the GbE2 Interconnect Switch.

SCP is typically used to copy files securely from one machine to another. SCP uses SSH for encryption of data on the network. On a GbE2 Interconnect Switch, SCP is used to download and upload the switch configuration via secure channels. By default, SCP is disabled on the GbE2 Interconnect Switch.

The GbE2 Interconnect Switch implementation of SSH is based on version 1.5 and version 2.0, and supports SSH clients from version 1.0 through version 2.0. Client software can use SSH version 1 or version 2. The following SSH clients are supported:

- SSH 3.0.1 for Linux (freeware)
- SecureCRT® 4.1.8 (VanDyke Technologies, Inc.)
- OpenSSH\_3.9 for Linux (FC 3)
- FedoraCore 3 for SCP commands
- PuTTY Release 0.58 (Simon Tatham) for Windows

## Configuring SSH and SCP features (CLI example)

Before you can use SSH commands, use the following commands to turn on SSH and SCP.

### Enabling or disabling SSH

To enable or disable the SSH feature, connect to the GbE2 Interconnect Switch CLI and enter the following commands:

```
>> # /cfg/sys/sshd/on                                (Turn SSH on)
Current status: OFF
New status: ON
>> # /cfg/sys/sshd/off                               (Turn SSH off)
Current status: OFF
New status: ON
```



**NOTE:** Secure Shell can be configured using the console port only. SSH menus do not display if you access the GbE2 Interconnect Switch using Telnet or the Browser-Based Interface.

### Enabling or disabling SCP apply and save

Enter the following commands from the GbE2 Interconnect Switch CLI to enable the SCP **putcfg\_apply** and **putcfg\_apply\_save** commands:

```
>> # /cfg/sys/sshd/ena                            (Enable SCP apply and save)
SSHD# apply                                         (Apply the changes to start generating RSA
host and server keys)
RSA host key generation starts
. . . . .
. . . . .
RSA host key generation completes (lasts 212549 ms)
RSA host key is being saved to Flash ROM, please don't reboot the box
immediately.
RSA server key generation starts
. . . . .
. . . . .
RSA server key generation completes (lasts 75503 ms)
RSA server key is being saved to Flash ROM, please don't reboot the box
immediately.
-----
Apply complete; don't forget to "save" updated configuration.
>> # /cfg/sys/sshd/dis                           (Disable SSH/SCP apply and save)
```

### Configuring the SCP administrator password

To configure the **scpadm** (SCP administrator) password, first connect to the GbE2 Interconnect Switch via the RS-232 management console. For security reasons, the **scpadm** password can be configured only when connected directly to the GbE2 Interconnect Switch console.

To configure the password, enter the following CLI command. At factory default settings, the current SCP administrator password is **admin**.

```
>> # /cfg/sys/sshd/scpadm
Changing SCP-only Administrator password; validation required. . .
Enter current administrator password: <password>
Enter new SCP-only administrator password: <new password>
Re-enter new SCP-only administrator password: <new password>
New SCP-only administrator password accepted.
```

## Using SSH and SCP client commands

The following shows the format for using some client commands. The examples below use 205.178.15.157 as the IP address of a sample GbE2 Interconnect Switch.

### Logging in to the GbE2 Interconnect Switch

Enter the following command to log in to the GbE2 Interconnect Switch:

```
ssh <user>@<switch IP address>
```

For example:

```
>> # ssh admin@205.178.15.157
```

### Downloading configuration from the GbE2 Interconnect Switch using SCP

Enter the following command to download the GbE2 Interconnect Switch configuration using SCP. You will be prompted for a password:

```
scp <user>@<switch IP address>:getcfg <local filename>
```

For example:

```
>> # scp admin@205.178.15.157:getcfg ad4.cfg
```

### Uploading configuration to the GbE2 Interconnect Switch using SCP

Enter the following command to upload configuration to the GbE2 Interconnect Switch. You will be prompted for a password.

```
scp <local filename> <user>@<switch IP address>:putcfg
```

For example:

```
>> # scp ad4.cfg admin@205.178.15.157:putcfg
```

### Applying and saving configuration

Enter the **apply** and **save** commands after the command above (**scp ad4.cfg 205.178.15.157:putcfg**), or use the following commands. You will be prompted for a password.

```
>> # scp <local_filename> <user>@<switch IP addr>:putcfg_apply  
>> # scp <local_filename> <user>@<switch IP addr>:putcfg_apply_save
```

For example:

```
>> # scp ad4.cfg admin@205.178.15.157:putcfg_apply  
>> # scp ad4.cfg admin@205.178.15.157:putcfg_apply_save
```

Note the following:

- The **diff** command is automatically executed at the end of **putcfg** to notify the remote client of the difference between the new and the current configurations.
- **putcfg\_apply** runs the **apply** command after the **putcfg** is done.
- **putcfg\_apply\_save** saves the new configuration to the flash after **putcfg\_apply** is done.
- The **putcfg\_apply** and **putcfg\_apply\_save** commands are provided because extra **apply** and **save** commands are usually required after a **putcfg**.

## SSH and SCP encryption of management messages

The following encryption and authentication methods are supported for SSH and SCP:

- Server Host Authentication—Client RSA authenticates the switch at the beginning of every connection
- Key Exchange—RSA
- Encryption—AES256-CBC, AES192-CBC, 3DES-CBC, 3DES, ARCFour
- User Authentication—Local password authentication, RADIUS, TACACS+



**IMPORTANT:** The SCP-only administrator password must be different from the regular administrator password.

### Generating RSA host and server keys for SSH access

To support the SSH server feature, two sets of RSA keys (host and server keys) are required. The host key is 1024 bits and is used to identify the GbE2 Interconnect Switch. The server key is 768 bits and is used to make it impossible to decipher a captured session by breaking into the GbE2 Interconnect Switch at a later time.

When the SSH server is first enabled and applied, the GbE2 Interconnect Switch automatically generates the RSA host and server keys and is stored in the flash memory.

To configure RSA host and server keys, first connect to the GbE2 Interconnect Switch console connection (commands are not available via Telnet connection), and enter the following commands to generate them manually:

>> # /cfg/sys/sshd/hkeygen	(Generates the host key)
>> # /cfg/sys/sshd/skeygen	(Generates the server key)

These two commands take effect immediately without the need of an **apply** command.

When the GbE2 Interconnect Switch reboots, it will retrieve the host and server keys from the flash memory. If these two keys are not available in the flash memory and if the SSH server feature is enabled, the GbE2 Interconnect Switch automatically generates them during the system reboot. This process may take several minutes to complete.

The GbE2 Interconnect Switch can also automatically regenerate the RSA server key. To set the interval of RSA server key autogeneration, use the following command:

>> # /cfg/sys/sshd/intrval <number of hours (0-24)>
---

A value of 0 denotes that RSA server key autogeneration is disabled. When greater than 0, the GbE2 Interconnect Switch will auto generate the RSA server key every specified interval; however, RSA server key generation is skipped if the GbE2 Interconnect Switch is busy doing other key or cipher generation when the timer expires.

The GbE2 Interconnect Switch will perform only one session of key/cipher generation at a time. Thus, an SSH/SCP client will not be able to log in if the GbE2 Interconnect Switch is performing key generation at that time, or if another client has logged in immediately prior. Also, key generation will fail if an SSH/SCP client is logging in at that time.

### SSH/SCP integration with RADIUS and TACACS+ authentication

SSH/SCP is integrated with RADIUS and TACACS+ authentication. After the RADIUS or TACACS+ server is enabled on the GbE2 Interconnect Switch, all subsequent SSH authentication requests will be redirected to the specified RADIUS or TACACS+ servers for authentication. The redirection is transparent to the SSH clients.

## User access control

The GbE2 Interconnect Switch allows an administrator to define end user accounts that permit end users to perform limited actions on the switch. Once end user accounts are configured and enabled, the switch requires username/password authentication.

For example, an administrator can assign a user who can log into the switch and perform operational commands (effective only until the next switch reboot).

Passwords can be up to 128 characters in length for TACACS, RADIUS, Telnet, SSH, console, and BBI access.

If RADIUS authentication is used, the user password on the Radius server will override the user password on the GbE2 switch. Also note that the password-change command on the switch modifies *only* the “use switch” password and has no effect on the user password on the Radius server. RADIUS authentication and user password cannot be used concurrently to access the switch.

### Setting up user IDs

The administrator can configure up to 10 user accounts.

To configure an end-user account, perform the following steps:

1. Select a user ID to define.

```
>> # /cfg/sys/access/user/uid 1
```

2. Define the user name and password.

```
>> User ID 1 # name jane          (Assign name "jane" to user ID 1)  
Current user name:  
New user name: jane
```

3. Define the user access level. By default, the end user is assigned to the user access level. To change the user's access level, enter the user Class of Service (cos) command, and select one of the available options.

```
>> User ID 1 # cos <user|oper|admin>
```

4. Enable the user ID.

```
>> # /cfg/sys/access/user/uid <#>/ena
```

Once an end user account is configured and enabled, the user can login to the switch using the username/password combination. The level of switch access is determined by the user CoS for the account.

# Ports and trunking

## Introduction



**NOTE:** All conceptual diagrams and port mappings in this chapter are based on BL 20p G3 servers. If you are using a next generation server, then see the latest Quick Setup Instructions card for correct port mappings.

The first part of this chapter describes the different types of ports used on the GbE2 Interconnect Switch. This information is useful in understanding other applications described in this guide, from the context of the embedded switch/server environment.

For specific information on how to configure ports for speed, auto-negotiation, and duplex modes, see the port commands in the *HP ProLiant BL p-Class GbE2 Interconnect Switch Command Reference Guide*.

The second part of this chapter provides configuration background and examples for trunking multiple ports together. Trunk groups can provide super-bandwidth, multi-link connections between GbE2 Interconnect Switches or other trunk-capable devices. A trunk group is a group of links that act together, combining their bandwidth to create a single, larger virtual link. The GbE2 Interconnect Switch provides trunking support for the six external ports, two crosslink ports, and 16 server ports.

## Ports on the GbE2 Interconnect Switch

The following table describes the Ethernet ports of the GbE2 Interconnect Switch, including the port name and function.



**NOTE:** The actual mapping of switch ports to NIC interfaces is dependant on the operating system software, the type of server blade, and the enclosure type. For more information, see the *HP ProLiant BL p-Class GbE2 Interconnect Switch User Guide*.

**Table 6** Ethernet switch port names

Port number	LED	Port alias
1	P1	Downlink1
2	P2	Downlink2
3	P3	Downlink3
4	P4	Downlink4
5	P5	Downlink5
6	P6	Downlink6
7	P7	Downlink7
8	P8	Downlink8
9	P9	Downlink9
10	P10	Downlink10
11	P11	Downlink11
12	P12	Downlink12
13	P13	Downlink13
14	P14	Downlink14
15	P15	Downlink15
16	P16	Downlink16
17	P17	XConnect1
18	P18	XConnect2
19	P19	Uplink1
20	P20	Uplink2

**Table 6** Ethernet switch port names

Port number	LED	Port alias
21	P21	Uplink3
22	P22	Uplink4
23	P23	FrontPanel1
24	P24	FrontPanel2

## Port trunk groups

When using port trunk groups between two GbE2 Interconnect Switches, you can create an aggregate link operating at up to four Gigabits per second, depending on how many physical ports are combined. The GbE2 Interconnect Switch supports up to 12 trunk groups per switch, each with up to six ports per trunk group.

The trunking software detects mis-configured (or broken) trunk links and redirects traffic on the mis-configured or broken trunk link to other trunk members within that trunk. You can only use trunking if each link has the same configuration for speed, flow control, and auto-negotiation.

## Statistical load distribution

In a configured trunk group containing more than one port, the load distribution is determined by information embedded within the data frame. For broadcast, multicast traffic, and unknown unicast packets, the lowest port number in the trunk group is elected to be the port for forwarding traffic. For IP traffic, the GbE2 Interconnect Switch will calculate the trunk port to use for forwarding traffic by implementing the load distribution algorithm on value equals to modulus of (XOR of last 3 bits of Source and last 3 bits of Destination IP address). For non-IP traffic, the GbE2 Interconnect Switch will calculate the trunk port to use for forwarding traffic by implementing the load distribution algorithm on value equals to modulus of (XOR of last 3 bits of Source and last 3 bits of Destination MAC address).

Multicast, broadcast, and unknown unicast are forwarded on the first STP port in the trunk group that comes online (usually the lowest port number in the trunk). If that link in the trunk fails, the next link (lowest port number) in the trunk is used. If the link is restored, traffic will not be re-routed to the lowest link until the current link fails again.

## Built-in fault tolerance

Since each trunk group is composed of multiple physical links, the trunk group is inherently fault tolerant. As long as even one physical link between the switches is available, the trunk remains active.

Statistical load distribution is maintained whenever a link in a trunk group is lost or returned to service.

## Before you configure trunks

When you create and enable a trunk, the trunk members (GbE2 Interconnect Switch ports) take on certain settings necessary for correct operation of the trunking feature.

Before you configure your trunk, you must consider these settings, along with specific configuration rules, as follows:

1. Read the configuration rules provided in the “Trunk Group Configuration Rules” section.
2. Determine which GbE2 Interconnect Switch ports (up to six) are to become trunk members (the specific ports making up the trunk).
3. Ensure that the chosen GbE2 Interconnect Switch ports are set to enabled, using the /cfg/port command.
4. Trunk member ports must have the same VLAN configuration.
5. Consider how the existing spanning tree will react to the new trunk configuration. See the “Spanning Tree Protocol” chapter for spanning tree group configuration guidelines.
6. Consider how existing VLANs will be affected by the addition of a trunk.

## Trunk group configuration rules

The trunking feature operates according to specific configuration rules. When creating trunks, consider the following rules that determine how a trunk group reacts in any network topology:

- All trunks must originate from one device, and lead to one destination device. For example, you cannot combine a link from Server 1 and a link from Server 2 into one trunk group.
- Any physical switch port can belong to only one trunk group.
- Trunking from non-HP devices must comply with Cisco® EtherChannel® technology.
- All trunk member ports must be assigned to the same VLAN configuration before the trunk can be enabled.
- All trunk member ports must be set to full duplex mode.
- All trunk member ports must be configured for the same speed.
- If you change the VLAN settings of any trunk member, you cannot apply the change until you change the VLAN settings of all trunk members.
- When an active port is configured in a trunk, the port becomes a trunk member when you enable the trunk using the /cfg/12/trunk/ena command. The spanning tree parameters for the port then change to reflect the new trunk settings.
- All trunk members must be in the same spanning tree group and can belong to only one spanning tree group. However if all ports are tagged, then all trunk ports can belong to multiple spanning tree groups.
- When a trunk is enabled, the trunk spanning tree participation setting takes precedence over that of any trunk member.
- You cannot configure a trunk member as a monitor port in a Port Mirroring configuration.
- A monitor port cannot monitor trunks; however, trunk members can be monitored.

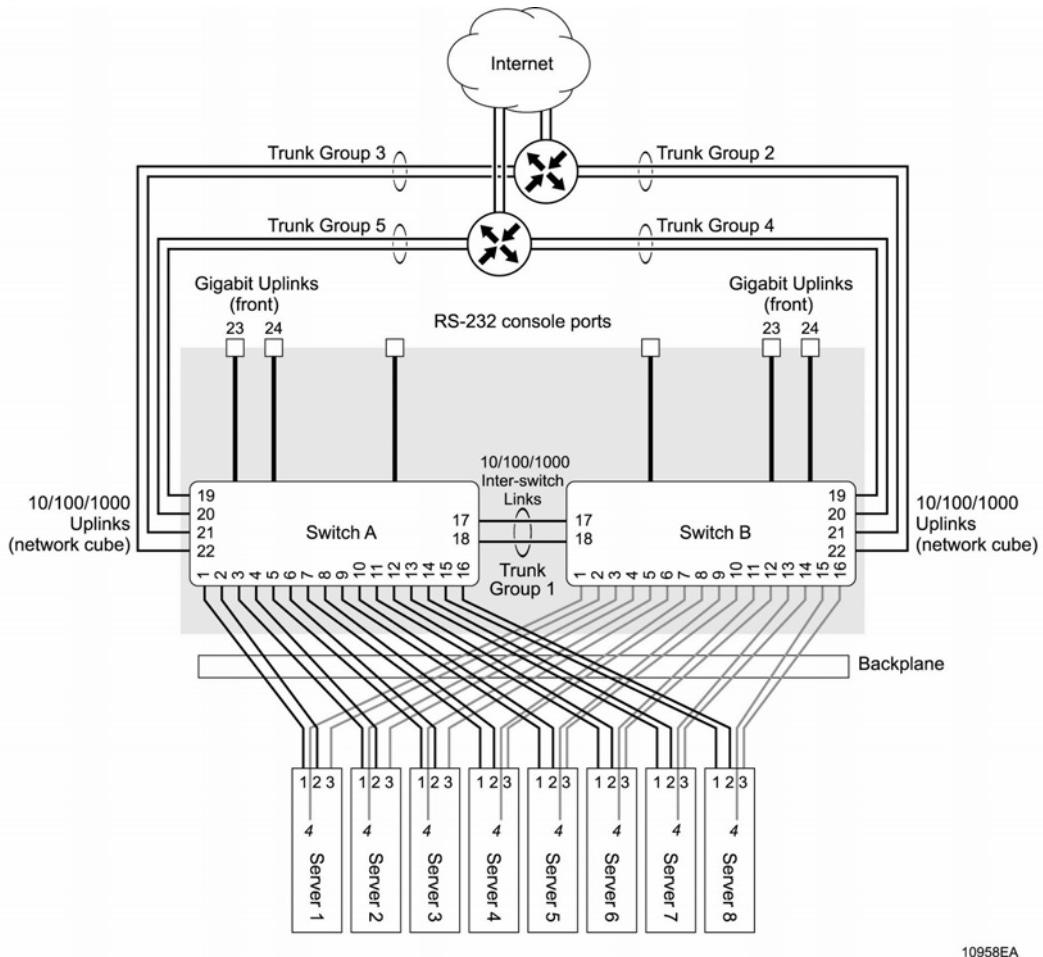
## Port trunking example

In this example, the Gigabit uplink ports on each GbE2 Interconnect Switch, and the crosslink ports are configured into a total of five trunk groups: two on each GbE2 Interconnect Switch, and one trunk group at the crosslink between the two GbE2 Interconnect Switches. All ports operate at Gigabit Ethernet speed.



**NOTE:** The actual mapping of switch ports to NIC interfaces is dependant on the operating system software, the type of server blade, and the enclosure type. For more information, see the *HP ProLiant BL p-Class GbE2 Interconnect Switch User Guide*.

**Figure 1** Port trunk group configuration example



10958EA

The trunk groups are configured as follows:

- Trunk group 1 is configured by default on the crosslink ports 17 and 18, which connect the GbE2 Interconnect Switches A and B together. Since this is the default configuration, you do not need to configure trunk group 1 on either GbE2 Interconnect Switch.
- Trunk groups 2-5 consist of two Gigabit uplink ports each, configured to act as a single link to the upstream routers. The trunk groups on each GbE2 Interconnect Switch are configured so that there is a link to each router for redundancy.

Prior to configuring each GbE2 Interconnect Switch in this example, you must connect to the appropriate switch CLI as the administrator. For details about accessing and using any of the commands described in this example, see the *HP ProLiant BL p-Class GbE2 Interconnect Switch Command Reference Guide*.

## Configuring trunk groups (CLI example)

1. On Switch A, configure trunk groups 5 and 3:

>> # /cfg/l2/trunk 5	(Select trunk group 5)
>> Trunk group 5# add 19	(Add port 19 to trunk group 5)
>> Trunk group 5# add 20	(Add port 20 to trunk group 5)
>> Trunk group 5# ena	(Enable trunk group 5)
>> Trunk group 5# apply	(Make your changes active)
>> # /cfg/l2/trunk 3	(Select trunk group 3)
>> Trunk group 3# add 21	(Add port 21 to trunk group 3)
>> Trunk group 3# add 22	(Add port 22 to trunk group 3)
>> Trunk group 3# ena	(Enable trunk group 3)
>> Trunk group 3# apply	(Make your changes active)
>> Trunk group 3# save	(Save for restore after reboot)

2. On Switch B, configure trunk groups 4 and 2:

>> # /cfg/l2/trunk 4	(Select trunk group 4)
>> Trunk group 4# add 19	(Add port 19 to trunk group 4)
>> Trunk group 4# add 20	(Add port 20 to trunk group 4)
>> Trunk group 4# ena	(Enable trunk group 4)
>> Trunk group 4# apply	(Make your changes active)
>> # /cfg/l2/trunk 2	(Select trunk group 2)
>> Trunk group 2# add 21	(Add port 21 to trunk group 2)
>> Trunk group 2# add 22	(Add port 22 to trunk group 2)
>> Trunk group 2# ena	(Enable trunk group 2)
>> Trunk group 2# apply	(Make your changes active)
>> Trunk group 2# save	(Save for restore after reboot)



**NOTE:** In this example, two GbE2 Interconnect Switches are used. Any third-party device supporting link aggregation should be configured manually. Connection problems could arise when using automatic trunk group negotiation on the third-party device.

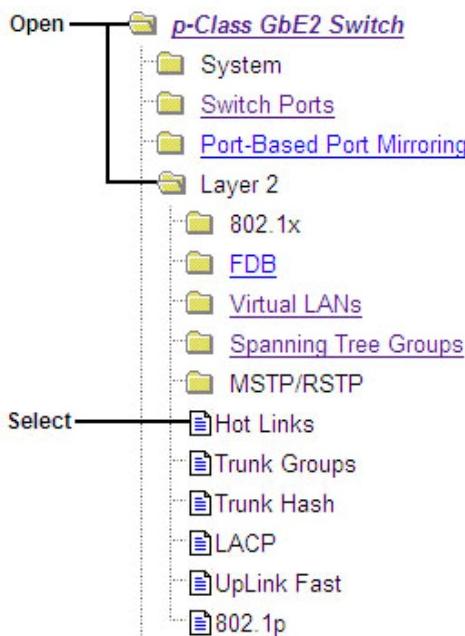
3. Examine the trunking information on each GbE2 Interconnect Switch using the following command:

>> /info/l2/trunk	(View trunking information)
-------------------	-----------------------------

Information about each port in each configured trunk group will be displayed. Make sure that trunk groups consist of the expected ports and that each port is in the expected state.

## Configuring trunk groups (BBI example)

1. Configure trunk groups.
  - a. Click the **Configure** context button on the Toolbar.
  - b. Open the Layer 2 folder, and select **Trunk Groups**.



- c. Click a Trunk Group number to select it.



Trunk Group	State
<a href="#">1</a>	enabled
<a href="#">2</a>	disabled
<a href="#">3</a>	disabled
<a href="#">4</a>	disabled
<a href="#">5</a>	disabled
<a href="#">6</a>	disabled
<a href="#">7</a>	disabled
<a href="#">8</a>	disabled
<a href="#">9</a>	disabled
<a href="#">10</a>	disabled
<a href="#">11</a>	disabled
<a href="#">12</a>	disabled

- d. Enable the Trunk Group. To add ports, select each port in the Ports Available list, and click **Add**.

### Switch Trunk Group 5 Configuration

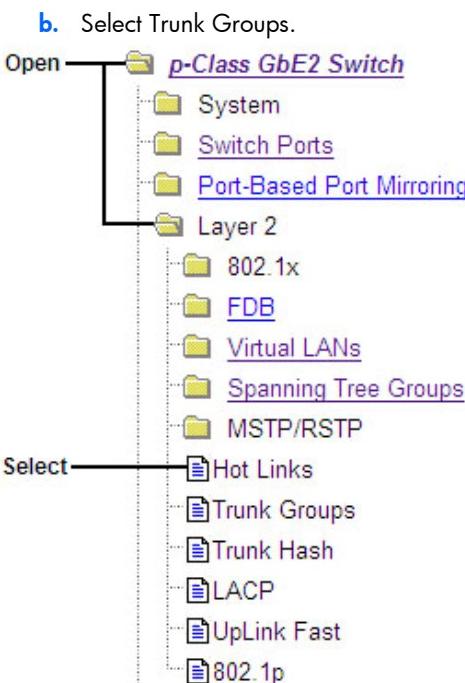
Trunk State	<input style="border: 1px solid black; padding: 2px 10px;" type="button" value="Enabled"/>				
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; vertical-align: top; padding-right: 20px;"> <b>Ports Available</b>    <div style="border: 1px solid #ccc; padding: 5px; width: 100%;"> Port15 <input type="checkbox"/>  Port16 <input type="checkbox"/>  Port21 <input type="checkbox"/>  Port22 <input type="checkbox"/>  Port23 <input type="checkbox"/> </div> </td> <td style="width: 50%; vertical-align: top;"> <b>Ports added to Trunk</b>    <div style="border: 1px solid #ccc; padding: 5px; width: 100%; background-color: #f0f0f0;"> PortID  Port19 <input checked="" type="checkbox"/>  Port20 <input checked="" type="checkbox"/> </div> </td> </tr> <tr> <td style="text-align: center; padding-top: 10px;"> <input style="border: 1px solid black; padding: 2px 10px;" type="button" value="Add&gt;&gt;"/>  <input style="border: 1px solid black; padding: 2px 10px;" type="button" value="&lt;&lt;Remove"/> </td> <td style="text-align: center; padding-top: 10px;"> <input style="border: 1px solid black; padding: 2px 10px;" type="button" value="Submit"/>  <input style="border: 1px solid black; padding: 2px 10px;" type="button" value="Delete"/> </td> </tr> </table>		<b>Ports Available</b>  <div style="border: 1px solid #ccc; padding: 5px; width: 100%;"> Port15 <input type="checkbox"/>  Port16 <input type="checkbox"/>  Port21 <input type="checkbox"/>  Port22 <input type="checkbox"/>  Port23 <input type="checkbox"/> </div>	<b>Ports added to Trunk</b>  <div style="border: 1px solid #ccc; padding: 5px; width: 100%; background-color: #f0f0f0;"> PortID  Port19 <input checked="" type="checkbox"/>  Port20 <input checked="" type="checkbox"/> </div>	<input style="border: 1px solid black; padding: 2px 10px;" type="button" value="Add&gt;&gt;"/> <input style="border: 1px solid black; padding: 2px 10px;" type="button" value="&lt;&lt;Remove"/>	<input style="border: 1px solid black; padding: 2px 10px;" type="button" value="Submit"/> <input style="border: 1px solid black; padding: 2px 10px;" type="button" value="Delete"/>
<b>Ports Available</b>  <div style="border: 1px solid #ccc; padding: 5px; width: 100%;"> Port15 <input type="checkbox"/>  Port16 <input type="checkbox"/>  Port21 <input type="checkbox"/>  Port22 <input type="checkbox"/>  Port23 <input type="checkbox"/> </div>	<b>Ports added to Trunk</b>  <div style="border: 1px solid #ccc; padding: 5px; width: 100%; background-color: #f0f0f0;"> PortID  Port19 <input checked="" type="checkbox"/>  Port20 <input checked="" type="checkbox"/> </div>				
<input style="border: 1px solid black; padding: 2px 10px;" type="button" value="Add&gt;&gt;"/> <input style="border: 1px solid black; padding: 2px 10px;" type="button" value="&lt;&lt;Remove"/>	<input style="border: 1px solid black; padding: 2px 10px;" type="button" value="Submit"/> <input style="border: 1px solid black; padding: 2px 10px;" type="button" value="Delete"/>				

- e. Click **Submit**.

2. Apply, verify, and save the configuration.



3. Examine the trunking information on each switch.  
a. Click the **Dashboard** context button on the Toolbar.



- c. Information about each configured trunk group is displayed. Make sure that trunk groups consist of the expected ports and that each port is in the expected state.

Switch Trunk Groups Dashboard		
Status	Trunk Group	Switch Port
	1	17
	1	18
	5	19
	5	20

## Configurable Trunk Hash algorithm

This feature allows you to configure the particular parameters for the GbE2 Trunk Hash algorithm instead of having to utilize the defaults. You can configure new default behavior for Layer 2 traffic and Layer 3 traffic, using the CLI menu `cfg/12/thash`. You can select a minimum of one or a maximum of two parameters to create one of the following configurations:

- Source IP (SIP)
- Destination IP (DIP)
- Source MAC (SMAC)
- Destination MAC (DMAC)
- Source IP (SIP) + Destination IP (DIP)
- Source MAC (SMAC) + Destination MAC (DMAC)

## Link Aggregation Control Protocol

Link Aggregation Control Protocol (LACP) is an IEEE 802.3ad standard for grouping several physical ports into one logical port (known as a dynamic trunk group or Link Aggregation group) with any device that supports the standard. Refer to the IEEE 802.3ad-2002 for a full description of the standard.

The 802.3ad standard allows standard Ethernet links to form a single Layer 2 link using the Link Aggregation Control Protocol (LACP). Link aggregation is a method of grouping physical link segments of the same media type and speed in full duplex, and treating them as if they were part of a single, logical link segment. If a link in a LACP trunk group fails, traffic is reassigned dynamically to the remaining link/s of the dynamic trunk group.



**NOTE:** Currently, LACP implementation does not support the Churn machine, an option used to detect if the port is operable within a bounded time period between the actor and the partner. Only the Market Responder is implemented, and there is no marker protocol generator.

A port's Link Aggregation Identifier (LAG ID) determines how the port can be aggregated. The Link Aggregation ID (LAG ID) is constructed mainly from the `system ID` and the port's `admin key`, as follows:

- **System ID**—The system ID is an integer value based on the switch's MAC address and the system priority assigned in the CLI.
- **Admin key**—A port's Admin key is an integer value (1-65535) that you can configure in the CLI. Each GbE2 port that participates in the same LACP trunk group must have the same `admin key` value. The Admin key is *local significant*, which means the partner switch does not need to use the same Admin key value.

For example, consider two switches, an Actor (the GbE2) and a Partner (another switch), as shown in the following table:

**Table 7** Actor vs. partner LACP configuration

Actor Switch	Partner Switch 1	Partner Switch 2
Port 19 (admin key = 100)	Port 1 (admin key = 50)	
Port 20 (admin key = 100)	Port 2 (admin key = 50)	
Port 21 (admin key = 200)		Port 3 (admin key = 60)
Port 22 (admin key = 200)		Port 4 (admin key = 60)

In the configuration shown in the table above, Actor switch ports 19 and 20 aggregate to form an LACP trunk group with Partner switch ports 1 and 2. At the same time, Actor switch ports 21 and 22 form a different LACP trunk group with a different partner.

LACP automatically determines which member links can be aggregated and then aggregates them. It provides for the controlled addition and removal of physical links for the link aggregation.

Each port in the GbE2 can have one of the following LACP modes.

- off (default)—The user can configure this port in to a regular static trunk group.
- active—The port is capable of forming an LACP trunk. This port sends LACPDU packets to partner system ports.
- passive—The port is capable of forming an LACP trunk. This port only responds to the LACPDU packets sent from an LACP active port.

Each active LACP port transmits LACP data units (LACPDUs), while each passive LACP port listens for LACPDUs. During LACP negotiation, the admin key is exchanged. The LACP trunk group is enabled as long as the information matches at both ends of the link. If the admin key value changes for a port at either end of the link, that port's association with the LACP trunk group is lost.

When the system is initialized, all ports by default are in LACP off mode and are assigned unique *admin keys*. To make a group of ports aggregatable, you assign them all the same *admin key*. You must set the port's LACP mode to active to activate LACP negotiation. You can set other port's LACP mode to passive, to reduce the amount of LACPDU traffic at the initial trunk-forming stage.

Use the /info/12/trunk command or the /info/12/lacp/dump command to check whether the ports are trunked.



**NOTE:** If you configure LACP on ports with 802.1x network access control, make sure the ports on both sides of the connection are properly configured for both LACP and 802.1x.

## Configuring LACP

Use the following procedure to configure LACP for port 19 and port 20 to participate in link aggregation.

1. Set the LACP mode on port 19.

```
>> # /cfg/12/lacp/port 19 (Select port 19)
>> LACP port 19# mode active (Set port 19 to LACP active mode)
```

2. Define the admin key on port 19. Only ports with the same admin key can form a LACP trunk group.

```
>> LACP port 19# adminkey 100          (Set port 19 adminkey to 100)
Current LACP port adminkey:      17
New pending LACP port adminkey: 100
```

3. Set the LACP mode on port 20.

```
>> # /cfg/12/lacp/port 20          (Select port 20)
>> LACP port 20# mode active      (Set port 20 to LACP active mode)
```

4. Define the admin key on port 20.

```
>> LACP port 20# adminkey 100          (Set port 20 adminkey to 100)
Current LACP port adminkey:      18
New pending LACP port adminkey: 100
```

5. Apply and verify the configuration.

>> LACP port 20# apply >> LACP port 20# cur	(Make your changes active) (View current trunking configuration)
--	---

6. Save your new configuration changes.

>> LACP port 20# save	(Save for restore after reboot)
-----------------------	---------------------------------

# Port-based Network Access and traffic control

## Port-based Network Access control

Port-based Network Access control provides a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics. It prevents access to ports that fail authentication and authorization. This feature provides security to all ports of the GbE2 Interconnect Switch.

The following topics are discussed in this section:

- Extensible Authentication Protocol over LAN
- 802.1x Authentication Process
- 802.1x Port States
- Supported RADIUS Attributes
- Configuration Guidelines

### Extensible authentication protocol over LAN

GbE2 Interconnect Switch software can provide user-level security for its ports using the IEEE 802.1x protocol, which is a more secure alternative to other methods of port-based network access control. Any device attached to an 802.1x-enabled port that fails authentication is prevented access to the network and denied services offered through that port.

The 802.1x standard describes port-based network access control using Extensible Authentication Protocol over LAN (EAPoL). EAPoL provides a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics and of preventing access to that port in cases of authentication and authorization failures.

EAPoL is a client-server protocol that has the following components:

- Supplicant or Client—The Supplicant is a device that requests network access and provides the required credentials (user name and password) to the Authenticator and the Authentication Server.
- Authenticator—The Authenticator enforces authentication and controls access to the network. The Authenticator grants network access based on the information provided by the Supplicant and the response from the Authentication Server. The Authenticator acts as an intermediary between the Supplicant and the Authentication Server: requesting identity information from the client, forwarding that information (encapsulated in RADIUS packets) to the Authentication Server for validation, relaying the server's responses to the client, and authorizing network access based on the results of the authentication exchange. The GbE2 Interconnect Switch acts as an Authenticator.
- Authentication Server,—The Authentication Server validates the credentials provided by the Supplicant to determine if the Authenticator should grant access to the network. The Authentication Server may be co-located with the Authenticator. The switch relies on external RADIUS servers for authentication.

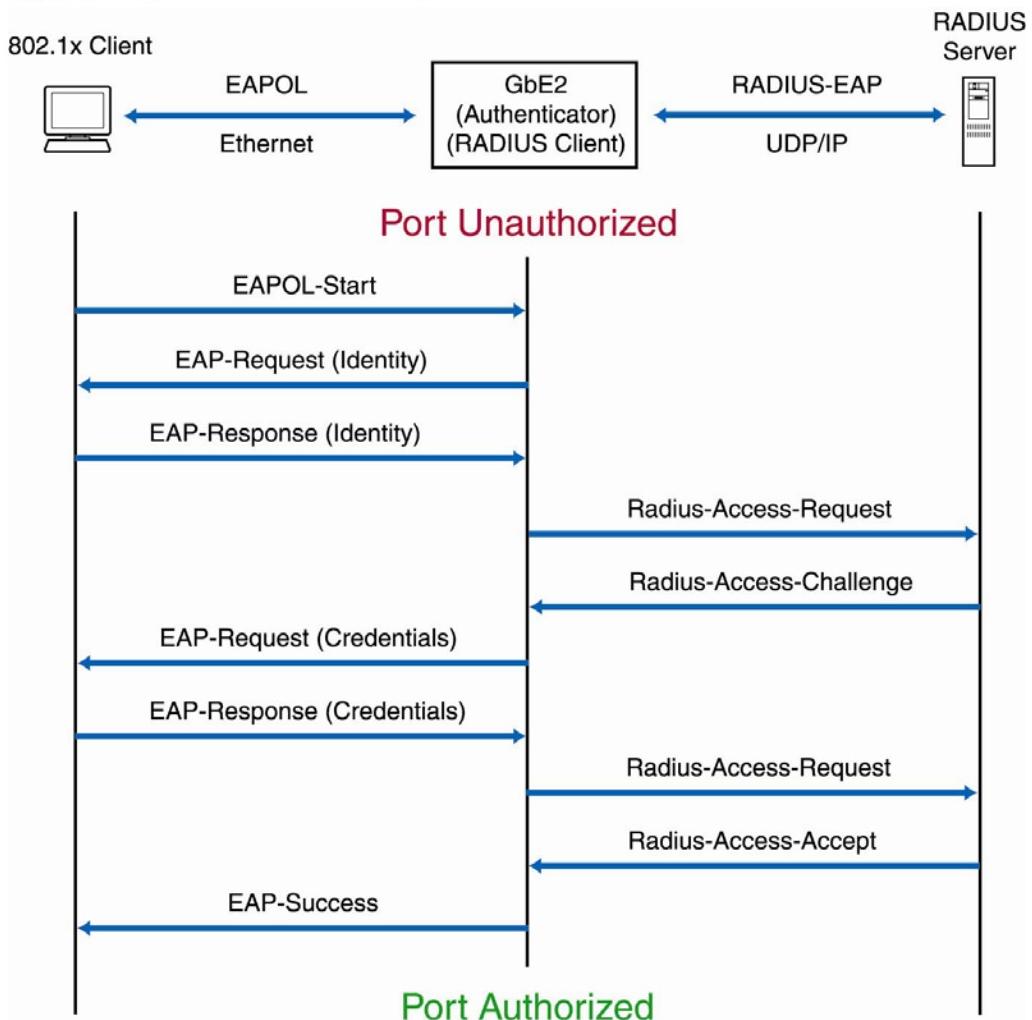
Upon a successful authentication of the client by the server, the 802.1x-controlled port transitions from unauthorized to authorized state, and the client is allowed full access to services through the port. When the client sends an EAP-Logoff message to the authenticator, the port will transition from authorized to unauthorized state.

### 802.1x authentication process

The clients and authenticators communicate using Extensible Authentication Protocol (EAP), which was originally designed to run over PPP, and for which the IEEE 802.1x Standard has defined an encapsulation method over Ethernet frames, called EAP over LAN (EAPoL).

The following figure shows a typical message exchange initiated by the client.

**Figure 2** Using EAPoL to authenticate a port



## EAPoL Message Exchange

During authentication, EAPoL messages are exchanged between the client and the switch authenticator, while RADIUS-EAP messages are exchanged between the switch authenticator and the Radius authentication server.

Authentication is initiated by one of the following methods:

Switch authenticator sends an EAP-Request/Identity packet to the client.

Client sends an EAPOL-Start frame to the switch authenticator, which responds with an EAP-Request/Identity frame.

The client confirms its identity by sending an EAP-Response/Identity frame to the switch authenticator, which forwards the frame encapsulated in a RADIUS packet to the server.

The Radius server chooses an EAP-supported authentication algorithm to verify the client's identity, and sends an EAP-Request packet to the client via the switch authenticator. The client then replies to the Radius server with an EAP-Response containing its credentials.

Upon a successful authentication of the client by the server, the 802.1x-controlled port transitions from unauthorized to authorized state, and the client is allowed full access to services through the controlled port. When the client later sends an EAPoL-Logoff message to the switch authenticator, the port transitions from authorized to unauthorized state.

If a client that does not support 802.1x connects to an 802.1x-controlled port, the switch authenticator requests the client's identity when it detects a change in the operational state of the port. The client does not respond to the request, and the port remains in the unauthorized state.



**NOTE:** When an 802.1x-enabled client connects to a port that is not 802.1x-controlled, the client initiates the authentication process by sending an EAPOL-Start frame. When no response is received, the client retransmits the request for a fixed number of times. If no response is received, the client assumes the port is in authorized state, and begins sending frames, even if the port is unauthorized.

## 802.1x port states

The state of the port determines whether the client is granted access to the network, as follows:

- **Unauthorized**—While in this state, the port discards all ingress and egress traffic except EAP packets.
- **Authorized**—When the client is authenticated successfully, the port transitions to the authorized state allowing all traffic to and from the client to flow normally.
- **Force Unauthorized**—You can configure this state that denies all access to the port.
- **Force Authorized**—You can configure this state that allows full access to the port.

Use the 802.1x Global Configuration Menu (/cfg/12/8021x/global) to configure 802.1x authentication for all ports in the switch. Use the 802.1x Port Menu (/cfg/12/8021x/port\_x) to configure a single port.

## Supported RADIUS attributes

The GbE 802.1x Authenticator relies on external RADIUS servers for authentication with EAP. The following table lists the RADIUS attributes that are supported as part of RADIUS-EAP authentication based on the guidelines specified in Annex D of the 802.1x standard and RFC 3580.

### Legend:

RADIUS Packet Types:

- A-R (Access-Request)
- A-A (Access-Accept)
- A-C (Access-Challenge)
- A-R (Access-Reject)

RADIUS Attribute Support:

- 0—This attribute MUST NOT be present in a packet.
- 0+—Zero or more instances of this attribute MAY be present in a packet.
- 0-1—Zero or one instance of this attribute MAY be present in a packet.
- 1—Exactly one instance of this attribute MUST be present in a packet.
- 1+—One or more of these attributes MUST be present.

**Table 8** EAP support for RADIUS attributes

#	Attribute	Attribute Value	A-R	A-A	A-C	A-R
1	User-Name	The value of the Type-Data field from the supplicant's EAP-Response/Identity message. If the Identity is unknown (i.e. Type-Data field is zero bytes in length), this attribute will have the same value as the Calling-Station-Id.	1	0-1	0	0
4	NAS-IP-Address	IP address of the authenticator used for RADIUS communication.	1	0	0	0
5	NAS-Port	Port number of the authenticator port to which the supplicant is attached.	1	0	0	0
24	State	Server-specific value. This is sent unmodified back to the server in an Access-Request that is in response to an Access-Challenge.	0-1	0-1	0-1	0
30	Called-Station-ID	The MAC address of the authenticator encoded as an ASCII string in canonical format, e.g. 000D5622E3 9F.	1	0	0	0

**Table 8** EAP support for RADIUS attributes

#	Attribute	Attribute Value	A-R	A-A	A-C	A-R
31	Calling-Station-ID	The MAC address of the supplicant encoded as an ASCII string in canonical format, e.g. 00034B436206.	1	0	0	0
79	EAP-Message	Encapsulated EAP packets from the supplicant to the authentication server (Radius) and vice-versa. The authenticator relays the decoded packet to both devices.	1+	1+	1+	1+
80	Message-Authenticator	Always present whenever an EAP-Message attribute is also included. Used to integrity-protect a packet.	1	1	1	1
87	NAS-Port-ID	Name assigned to the authenticator port, e.g. Server1_Port3	1	0	0	0

## EAPoL configuration guidelines

When configuring EAPoL, consider the following guidelines:

- The 802.1x port-based authentication is currently supported only in point-to-point configurations, that is, with a single supplicant connected to an 802.1x-enabled switch port.
- When 802.1x is enabled, a port has to be in the authorized state before any other Layer 2 feature can be operationally enabled. For example, the STG state of a port is operationally disabled while the port is in the unauthorized state.
- The 802.1x supplicant capability is not supported. Therefore, none of its ports can connect successfully to an 802.1x-enabled port of another device, such as another switch, that acts as an authenticator, unless access control on the remote port is disabled or is configured in forced-authorized mode. For example, if a GbE2 Interconnect switch is connected to another GbE2 Interconnect Switch, and if 802.1x is enabled on both switches, the two connected ports must be configured in force-authorized mode.
- The 802.1x standard has optional provisions for supporting dynamic virtual LAN assignment via RADIUS tunneling attributes, for example, Tunnel-Type (=VLAN), Tunnel-Medium-Type (=802), and Tunnel-Private-Group-ID (=VLAN id). These attributes are not supported and might affect 802.1x operations. Other unsupported attributes include Service-Type, Session-Timeout, and Termination-Action.

RADIUS accounting service for 802.1x-authenticated devices or users is not supported.

Configuration changes performed using SNMP and the standard 802.1x MIB take effect immediately.

## Port-based traffic control

Port-based traffic control prevents GbE2 Interconnect Switch ports from being disrupted by LAN storms. A LAN storm occurs when data packets flood the LAN, which can cause the network to become congested and slow down. Errors in the protocol-stack implementation or in the network configuration can cause a LAN storm.

You can enable port-based traffic control separately for each of the following traffic types:

- Broadcast—packets with destination MAC address ff:ff:ff:ff:ff:ff
- Multicast—packets that have MAC addresses with the least significant bit of their first octet set to one
- Destination Lookup Failed (DLF)—packets with unknown destination MAC address, that are treated like broadcast packets

With Port-based Traffic Control enabled, the port monitors incoming traffic of each type noted above. If the traffic exceeds a configured threshold, the port blocks traffic that exceeds the threshold until the traffic flow falls back within the threshold.

The GbE2 supports separate traffic-control thresholds for broadcast, multicast, and DLF traffic. The traffic threshold is measured in number of frames per second.



**NOTE:** All ports that belong to a trunk must have the same traffic-control settings.

## Configuring port-based traffic control

To configure a port for traffic control, perform the following steps:

1. Configure the traffic-control threshold and enable traffic control.

```
Main# /cfg/port 2
>> Port 2# brate 150000          (Set broadcast threshold)
>> Port 2# mrate 150000          (Set multicast threshold)
>> Port 2# drate 150000          (Set DLF threshold)
```

2. To disable a traffic-control threshold, use the following command:

```
>> Port 2# mrate dis           (Disable multicast threshold)
```

3. Apply and save the configuration.

```
>> Port 2# apply                (Apply the port configurations)
>> Port 2# save                 (Save the port configurations)
```

# VLANs

## Introduction

This chapter describes network design and topology considerations for using Virtual Local Area Networks (VLANs). VLANs are commonly used to split up groups of network users into manageable broadcast domains, to create logical segmentation of workgroups, and to enforce security policies among logical segments.

The following topics are discussed in this chapter:

- VLANs and Port VLAN ID Numbers
- VLAN Tagging
- VLANs and IP Interfaces
- VLAN Topologies and Design Considerations



**NOTE:** Basic VLANs can be configured during initial switch configuration.

More comprehensive VLAN configuration can be done from the command line interface. See the "VLAN configuration" and "Port configuration" sections in the *HP ProLiant BL p-Class GbE2 Interconnect Switch Command Reference Guide*.

## Overview

Setting up VLANs is a way to segment networks to increase network flexibility without changing the physical network topology. With network segmentation, each GbE2 Interconnect Switch port connects to a segment that is a single broadcast domain. When a GbE2 Interconnect Switch port is configured to be a member of a VLAN, it is added to a group of ports (workgroup) that belongs to one broadcast domain.

Ports are grouped into broadcast domains by assigning them to the same VLAN. Multicast, broadcast, and unknown unicast frames are flooded only to ports in the same VLAN.

## VLANs and port VLAN ID numbers

### VLAN numbers

The GbE2 Interconnect Switch supports up to 1,000 VLANs per switch. Even though the maximum number of VLANs supported at any given time is 1,000, each can be identified with any number between 1 and 4095. VLAN 1 is the default VLAN, and all ports are assigned to it.

### Viewing VLANs

The VLAN information menu (`/info/l2/vlan`) displays all configured VLANs and all member ports that have an active link state, for example:

>> Layer 2# vlan		Name	Status	Ports
1	Default VLAN		ena	1 4-22 24
2	VLAN 2		ena	2 3
4092	VLAN 4092		ena	23

### PVID numbers

Each port in the GbE2 Interconnect Switch has a configurable default VLAN number, known as its PVID. This places all ports on the same VLAN initially, although each port PVID is configurable to any VLAN number between 1 and 4095.

The default configuration settings for GbE2 Interconnect Switches have all ports set as untagged members of VLAN 1 with all ports configured as PVID = 1. In the default configuration example shown in the following figure, all incoming packets are assigned to VLAN 1 by the default port VLAN identifier (PVID =1).

## Viewing and configuring PVIDs

You can view PVIDs from the following CLI commands:

### Port information

Port	Tag	RMON	PVID	NAME	VLAN (s)
1	n	d	1	Downlink1	1
2	n	e	1	Downlink2	1
3	n	d	1	Downlink3	1
4	n	d	1	Downlink4	1
5	n	d	1	Downlink5	1
6	n	d	1	Downlink6	1
7	n	d	1	Downlink7	1
:					
:					

### Port configuration

```
>> /cfg/port 22/pvid 22
Current port VLAN ID:      1
New pending port VLAN ID: 22

>> Port 22#
```

Each port on the GbE2 Interconnect Switch can belong to one or more VLANs, and each VLAN can have any number of switch ports in its membership. Any port that belongs to multiple VLANs, however, must have VLAN tagging enabled. See the “VLAN tagging” section in this chapter.

Any untagged frames (those with no VLAN specified) are classified with the PVID of the sending port.

## VLAN tagging

The GbE2 Interconnect Switch supports IEEE 802.1Q VLAN tagging, providing standards-based VLAN support for Ethernet systems.

Tagging places the VLAN identifier in the frame header, allowing each port to belong to multiple VLANs. When you configure multiple VLANs on a port, you must also enable tagging on that port.

Since tagging fundamentally changes the format of frames transmitted on a tagged port, you must carefully plan network designs to prevent tagged frames from being transmitted to devices that do not support 802.1Q VLAN tags, or devices where tagging is not enabled.

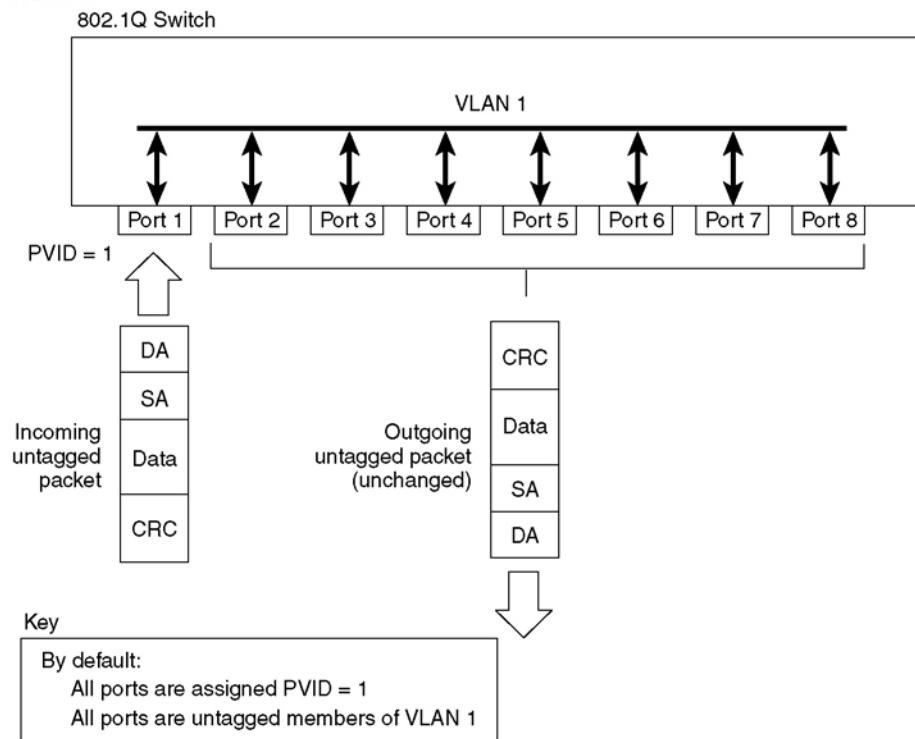
Important terms used with the 802.1Q tagging feature are:

- VLAN identifier (VID)—the 12-bit portion of the VLAN tag in the frame header that identifies an explicit VLAN.
- Port VLAN identifier (PVID)—a classification mechanism that associates a port with a specific VLAN. For example, a port with a PVID of 3 (PVID =3) assigns all untagged frames received on this port to VLAN 3.
- Tagged frame—a frame that carries VLAN tagging information in the header. The VLAN tagging information is a 32-bit field (VLAN tag) in the frame header that identifies the frame as belonging to a specific VLAN. Untagged frames are marked (tagged) with this classification as they leave the GbE2 Interconnect Switch through a port that is configured as a tagged port.
- Untagged frame—a frame that does not carry any VLAN tagging information in the frame header.
- Untagged member—a port that has been configured as an untagged member of a specific VLAN. When an untagged frame exits the GbE2 Interconnect Switch through an untagged member port, the frame header remains unchanged. When a tagged frame exits the GbE2 Interconnect Switch through an untagged member port, the tag is stripped and the tagged frame is changed to an untagged frame.
- Tagged member—a port that has been configured as a tagged member of a specific VLAN. When an untagged frame exits the GbE2 Interconnect Switch through a tagged member port, the frame header is modified to include the 32-bit tag associated with the PVID. When a tagged frame exits the GbE2 Interconnect Switch through a tagged member port, the frame header remains unchanged (original VID remains).



**NOTE:** If an 802.1Q tagged frame is sent to a port that has VLAN-tagging disabled, then the frames are forwarded based on their port-VLAN ID (PVID).

**Figure 3** Default VLAN settings



BS45010A

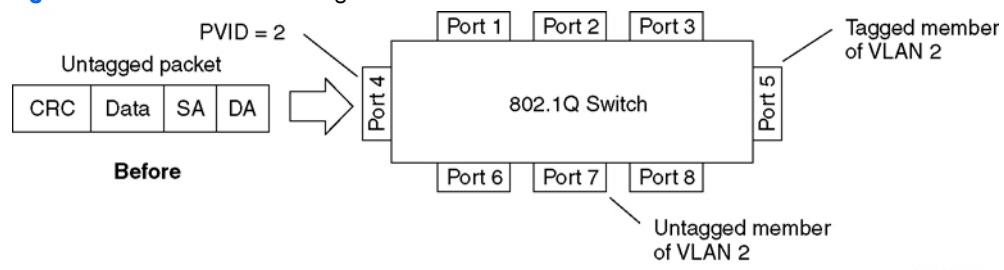


**NOTE:** The port numbers specified in these illustrations may not directly correspond to the physical port configuration of your GbE2 Interconnect Switch model.

When you configure VLANs, you configure the GbE2 Interconnect Switch ports as tagged or untagged members of specific VLANs. Refer to the following figures.

In the following figure, the untagged incoming packet is assigned directly to VLAN 2 (PVID = 2). Port 5 is configured as a tagged member of VLAN 2, and port 7 is configured as an untagged member of VLAN 2.

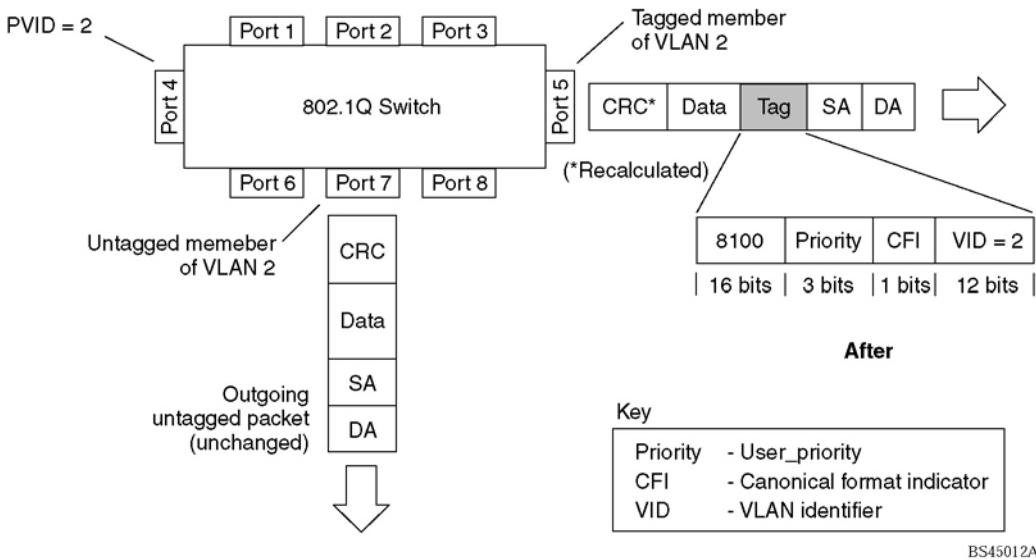
**Figure 4** Port-based VLAN assignment



BS45011A

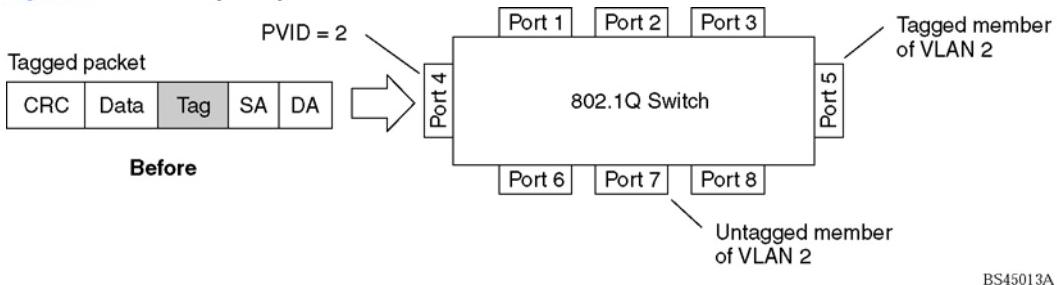
As shown in the following figure, the untagged packet is marked (tagged) as it leaves the GbE2 Interconnect Switch through port 5, which is configured as a tagged member of VLAN 2. The untagged packet remains unchanged as it leaves the GbE2 Interconnect Switch through port 7, which is configured as an untagged member of VLAN 2.

**Figure 5** 802.1Q tagging (after port-based VLAN assignment)



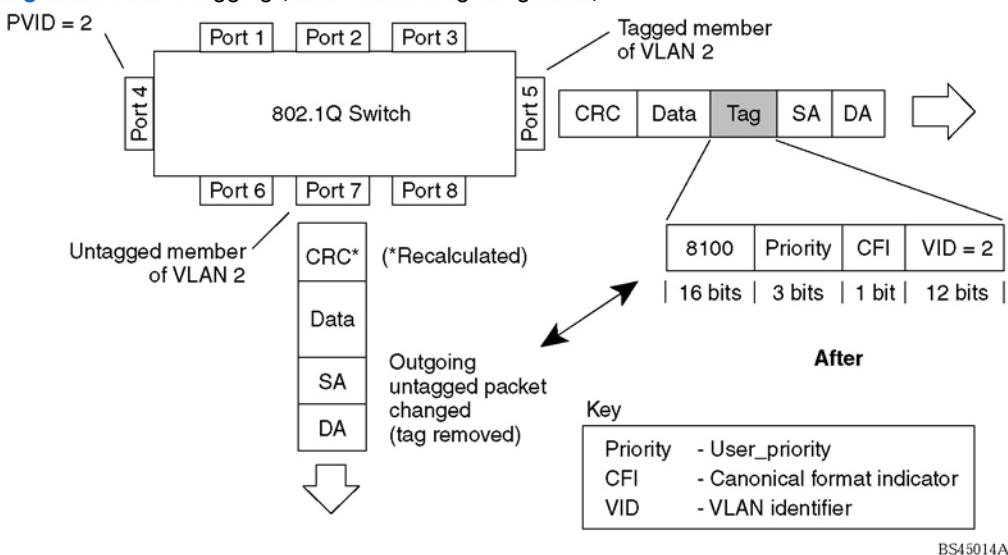
In the following figure, the tagged incoming packet is assigned directly to VLAN 2 because of the tag assignment in the packet. Port 5 is configured as a tagged member of VLAN 2, and port 7 is configured as an untagged member of VLAN 2.

**Figure 6** 802.1Q tag assignment



As shown in the following figure, the tagged packet remains unchanged as it leaves the GbE2 Interconnect Switch through port 5, which is configured as a tagged member of VLAN 2. However, the tagged packet is stripped (untagged) as it leaves the GbE2 Interconnect Switch through port 7, which is configured as an untagged member of VLAN 2.

**Figure 7** 802.1Q tagging (after 802.1Q tag assignment)



**NOTE:** Using the `/boot/conf factory` command resets all ports to VLAN 1 and all other settings to the factory defaults at the next reboot.

## VLANs and IP interfaces

Carefully consider how you create VLANs within the GbE2 Interconnect Switch, so that communication with the GbE2 Interconnect Switch remains possible. In order to access the GbE2 Interconnect Switch for remote configuration, trap messages, and other management functions, make sure that at least one IP interface on the GbE2 Interconnect Switch has a VLAN defined.

You can also inadvertently cut off access to management functions if you exclude the ports from the VLAN membership. For example, if all IP interfaces are left on VLAN 1 (the default), and all ports are configured for VLAN 2, then GbE2 Interconnect Switch management features are effectively cut off.

To remedy this, keep all ports used for remote GbE2 Interconnect Switch management on the default VLAN and assign an IP interface to the default VLAN.

For more information on configuring IP interfaces, see the “Configuring an IP interface” section in the “Accessing the GbE2 Interconnect Switch” chapter.

## VLAN topologies and design considerations

By default, all GbE2 Interconnect Switch ports are configured to the default VLAN 1. This configuration groups all ports into the same broadcast domain. The VLAN has an 802.1Q VLAN ID of 1. VLAN tagging is turned off, because by default all ports are members of a single VLAN only.

If configuring Spanning Tree Protocol (/cfg/12/stp), note that each of spanning tree groups 2-16 may contain only one VLAN. If configuring Multiple Spanning Tree Protocol (/cfg/12/mrst), each of spanning tree groups 1-16 may contain multiple VLANs.

## VLAN configuration rules

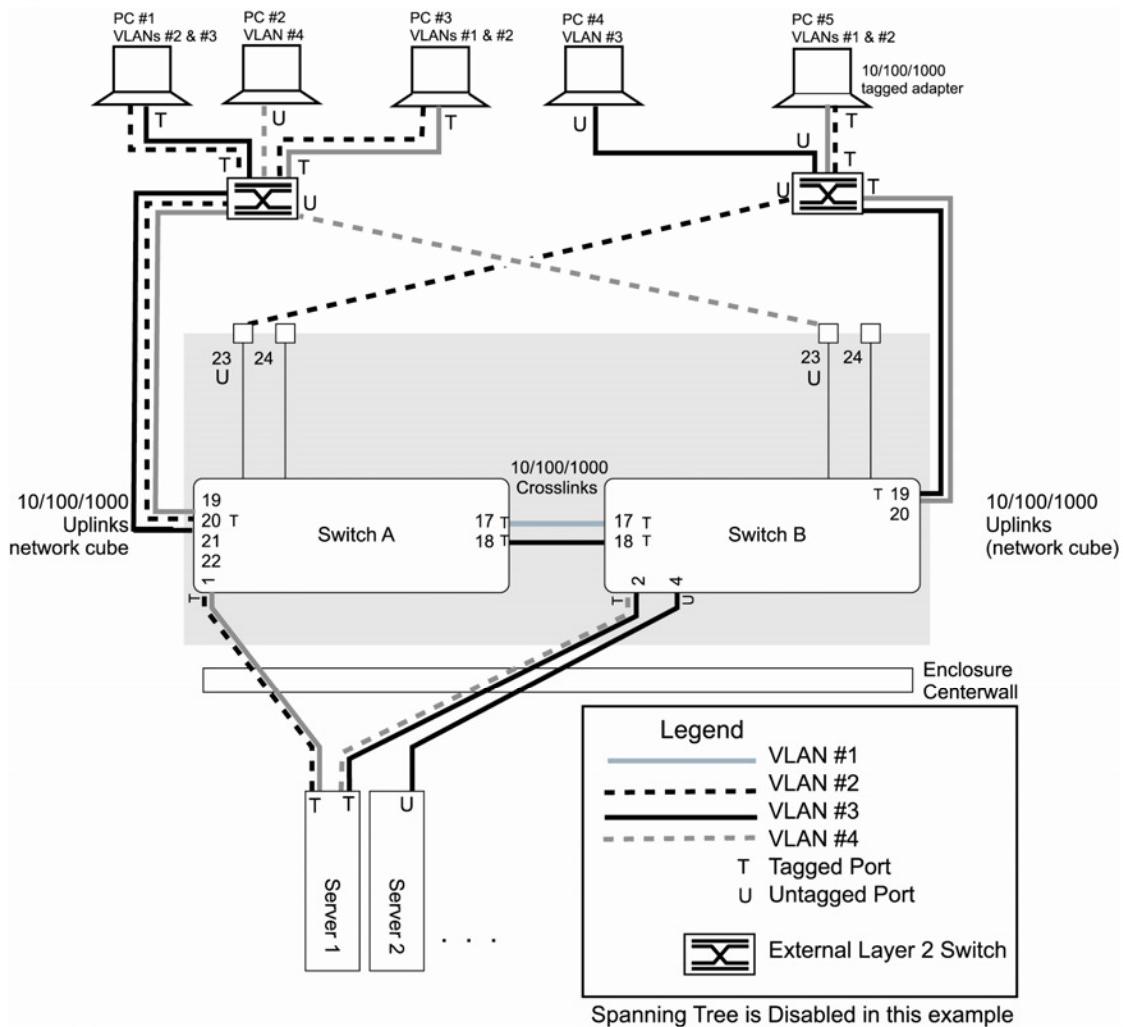
VLANs operate according to specific configuration rules which must be considered when creating VLANs. For example:

- HP recommends that all ports involved in trunking and Port Mirroring have the same VLAN configuration. If a port is on a trunk with a mirroring port, the VLAN configuration cannot be changed. For more information on port trunking, see the “Port Trunking example” section in the “Ports and trunking” chapter.
- All ports that are involved in Port Mirroring must have memberships in the same VLANs. If a port is configured for Port Mirroring, the port’s VLAN membership cannot be changed. For more information on configuring Port Mirroring, see the “Port Mirroring” section in the “Troubleshooting tools” appendix.
- When you delete a VLAN, untagged ports are moved to the default VLAN (VLAN 1). Tagged ports that belong only to the deleted VLAN are moved to the VLAN identified by the PVID. Tagged ports that belong to multiple VLANs are removed from the deleted VLAN only.

## Multiple VLANs with tagging

The following figure shows only those switch port to server links that must be configured for the example. While not shown, all other server links remain set at their default settings.

**Figure 8** Multiple VLANs with VLAN tagging



The features of this VLAN are described in the following table:

**Table 9** Multiple VLANs with tagging

Component	Description
Switch A	Switch A is configured for VLANS 1, 2, and 3. Port 1 is tagged to accept traffic from VLANs 1 and 2. Ports 17 and 18 are tagged members of a trunk that accepts traffic from VLANs 1 and 3. Port 20 is tagged to accept traffic from VLANs 1, 2, and 3. Port 23 is an untagged member of VLAN 2.
Switch B	Switch B is configured for VLANS 1, 3, and 4. Port 2 is tagged to accept traffic from VLANs 3 and 4. Port 4 is configured only for VLAN 3, so VLAN tagging is off.
Blade Server #1	This high-use blade server needs to be accessed from all VLANs and IP subnets. The server has a VLAN-tagging adapter installed with VLAN tagging turned on. One adapter is attached to one of the switch's 10/100/1000 Mbps ports, that is configured for VLANs 1 and 2. One adapter is configured for VLANs 3 and 4. Because of the VLAN tagging capabilities of both the adapter and the switch, the server is able to communicate on all four VLANs in this network while maintaining broadcast separation among all four VLANs and subnets.
Blade Server #2	This blade server belongs to VLAN 3. The port that the VLAN is attached to is configured only for VLAN 3, so VLAN tagging is off.
PC #1	This PC is a member of VLAN 2 and 3. Via VLAN 2, it can communicate with Server 1, PC 3, and PC 5. Via VLAN 3, it can communicate with Server 1, Server 2, and PC 4.
PC #2	This PC is a member of VLAN 4, and can only communicate with Server 1.
PC #3	This PC is a member of VLAN 1 and VLAN 2. Via VLAN 1, it can communicate with Server 1 and PC 5. Via VLAN 2, it can communicate with Server 1, PC 1, and PC 5.

**Table 9** Multiple VLANs with tagging

Component	Description
PC #4	This PC is a member of VLAN 3, and it can communicate with Server 1, Server 2, and PC 1.
PC #5	This PC is a member of both VLAN 1 and VLAN 2. Via VLAN 1, it can communicate with Server 1 and PC 3. Via VLAN 2, it can communicate with Server 1, PC 1, and PC 3. The Layer 2 switch port to which it is connected is configured for both VLAN 1 and VLAN 2 and has tagging enabled.



**NOTE:** All PCs connected to a tagged port must have a Gigabit Ethernet adapter with VLAN-tagging capability installed.

## Configuring the example network

These examples describe how to configure ports and VLANs on Switch A and Switch B.

### Configuring ports and VLANs on Switch A (CLI example)

To configure ports and VLANs on Switch A, do the following:

1. On Switch A, enable VLAN tagging on the necessary ports.

```
Main# /cfg/port 1                                     (Select port 1: connection to server 1)
>> Port 1# tag e

Current VLAN tag support: disabled
New VLAN tag support:     enabled                  (Enable tagging)
Port 1 changed to tagged.

Main# /cfg/port 17                                    (Select crosslink link port 17)
>> Port 17# tag e

Current VLAN tag support: disabled
New VLAN tag support:     enabled                  (Enable tagging)
Port 17 changed to tagged.

Main# /cfg/port 18                                    (Select crosslink link port 18)
>> Port 18# tag e

Current VLAN tag support: disabled
New VLAN tag support:     enabled                  (Enable tagging)
Port 18 changed to tagged.

Main# /cfg/port 20                                     (Select uplink port 20)
>> Port 20# tag e

Current VLAN tag support: disabled
New VLAN tag support:     enabled
Port 20 changed to tagged.

>> Port 20# apply                                     (Apply the port configurations)
```

2. Configure the VLANs and their member ports. Since all ports are by default configured for VLAN 1, configure only those ports that belong to VLAN 2. crosslink ports 17 and 18 must belong to VLANs 1 and 2.

```

>> /cfg/l2/vlan 2
>> VLAN 2# add 1
Current ports for VLAN 2: empty
Pending new ports for VLAN 2: 1
                                         (Add port 1 to VLAN 2)

>> VLAN 2# add 20
Current ports for VLAN 2: 1
Pending new ports for VLAN 2: 20
                                         (Add port 20 to VLAN 2)

>> VLAN 2# add 23
Port 23 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]: y
Current ports for VLAN 2: 1, 20
Pending new ports for VLAN 2: 23
                                         (Add port 23 to VLAN 2)

>> /cfg/l2/vlan 3
>> VLAN 3# add 17
Current ports for VLAN 3: empty
Pending new ports for VLAN 3: 17
                                         (Add port 17 to VLAN 3)

>> VLAN 3# add 18
Current ports for VLAN 3: 17
Pending new ports for VLAN 3: 18
                                         (Add port 18 to VLAN 3)

>> VLAN 3# add 20
Current ports for VLAN 3: 17, 18
Pending new ports for VLAN 3: 20
                                         (Add port 20 to VLAN 3)

>> apply
                                         (Apply the port configurations)
>> save
                                         (Save the port configurations)

```

## Configuring ports and VLANs on Switch B (CLI example)

To configure ports and VLANs on Switch B, do the following:

- On Switch B, enable VLAN tagging on the necessary ports. Port 4 (connection to server 2) remains untagged, so it is not configured below.

```

Main# /cfg/port 2
                                         (Select port 2: connection to server 1)
>> Port 2# tag e
Current VLAN tag support: disabled
New VLAN tag support: enabled
Port 2 changed to tagged.

Main# /cfg/port 17
                                         (Select crosslink link port 17)
>> Port 17# tag e
                                         (Enable tagging)
Current VLAN tag support: disabled
New VLAN tag support: enabled
Port 17 changed to tagged.

Main# /cfg/port 18
                                         (Select crosslink link port 18)
>> Port 18# tag e
                                         (Enable tagging)
Current VLAN tag support: disabled
New VLAN tag support: enabled
Port 18 changed to tagged.

Main# /cfg/port 19
                                         (Select uplink port 19)
>> Port 19# tag e
                                         (Enable tagging)
Current VLAN tag support: disabled
New VLAN tag support: enabled
Port 19 changed to tagged.
>> Port 19# apply
                                         (Apply the port configurations)

```

- Configure the VLANs and their member ports. Since all ports are by default configured for VLAN 1, configure only those ports that belong to other VLANs.

```

>> /cfg/l2/vlan 3
>> VLAN 3# add 2
Current ports for VLAN 3: empty
Pending new ports for VLAN 3: 2

>> VLAN 3# add 17
Current ports for VLAN 3: 2, 4
Pending new ports for VLAN 3: 17

>> VLAN 3# add 18
Current ports for VLAN 3: 2, 17
Pending new ports for VLAN 3: 18

>> VLAN 3# add 19
Current ports for VLAN 3: 2, 17, 18
Pending new ports for VLAN 3: 19

>> /cfg/l2/vlan 4
>> VLAN 4# add 2
Current ports for VLAN 4: empty
Pending new ports for VLAN 4: 2

>> VLAN 4# add 4
Port 4 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 4 [y/n]: y
Current ports for VLAN 4: 2
Pending new ports for VLAN 4: 4

>> VLAN 4# add 23
Port 23 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 4 [y/n]: y
Current ports for VLAN 4: 2, 4
Pending new ports for VLAN 4: 23

>> apply                                     (Apply the port configurations)
>> save                                      (Save the port configurations)

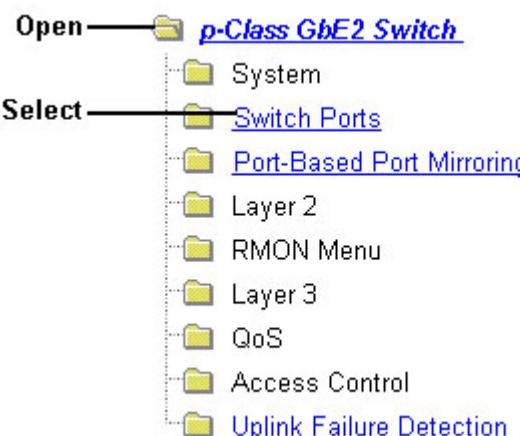
```

The external Layer 2 switches should also be configured for VLANs and tagging.

## Configuring ports and VLANs on Switch A (BBI example)

To configure ports and VLANs on Switch A, do the following:

- On the HP ProLiant BL p-Class GbE2 Interconnect Switch A, enable VLAN tagging on the necessary ports.
  - Click the **Configure** context button on the Toolbar.
  - Open the Switch folder, and select **Switch Ports** (click the underlined text, not the folder).



- c. Click a port number to select it.

Switch Port	State	VLAN Tagging	Default PVID	PVID tagging	Multicast Threshold	Broadcast Threshold	Destination Lookup Fail Threshold	802.1p Priority
Select ————— <a href="#">1</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0
<a href="#">2</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0
<a href="#">3</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0
<a href="#">4</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0
<a href="#">5</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0
<a href="#">6</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0
<a href="#">7</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0
<a href="#">8</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0
<a href="#">9</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0
<a href="#">10</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0

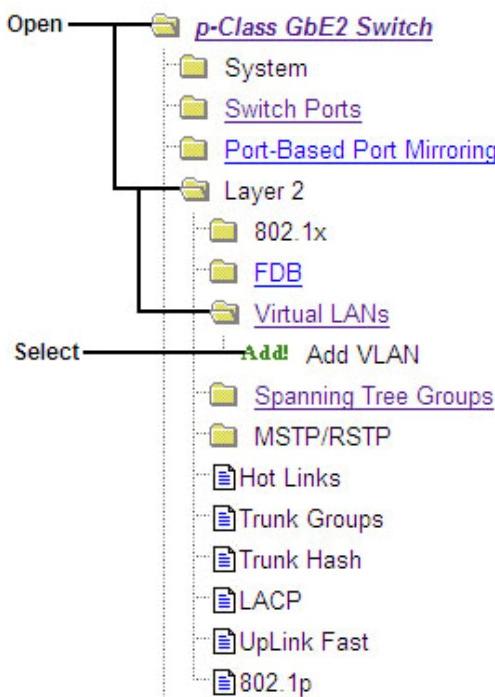
- d. Enable the port and enable VLAN tagging.

Switch Port 1 Configuration

Switch Port State	Enabled <input type="button" value="▼"/>
RMON Instrumentation	Disabled <input type="button" value="▼"/>
VLAN Tagging	Enabled <input type="button" value="▼"/>
PVID Tagging	Enabled <input type="button" value="▼"/>
Port STP	On <input type="button" value="▼"/>
Default Port VLAN ID (1 - 4095)	1
Flow Control	both Rx/Tx <input type="button" value="▼"/>
Autonegotiation	Enabled <input type="button" value="▼"/>
Speed	10/100/1000 <input type="button" value="▼"/>
Duplex Mode	Full/Half <input type="button" value="▼"/>
Enable/Disable sending Link UP/Down Trap	Enabled <input type="button" value="▼"/>
Port Name	Downlink1

- e. Click **Submit**.

2. Configure the VLANs and their member ports.
- Open the Virtual LANs folder, and select **Add VLAN**.



- Enter the VLAN name, VLAN ID number, and enable the VLAN. To add ports, select each port in the Ports Available list and click **Add**. Since all ports are configured for VLAN 1 by default, configure only those ports that belong to VLAN 2. The crosslink ports 17 and 18 must belong to VLANs 1 and 2.

**VLAN "New" Configuration**

VLAN Name	VLAN Example
VLAN ID (1 - 4095) From	2
VLAN State	enabled
Spanning Tree Group	2

**Ports Available**

Port:ID  
Port:2  
Port:3  
Port:4  
Port:5  
Port:6  
Port:7  
Port:8  
Port:9  
Port:10

**Ports in Vlan**

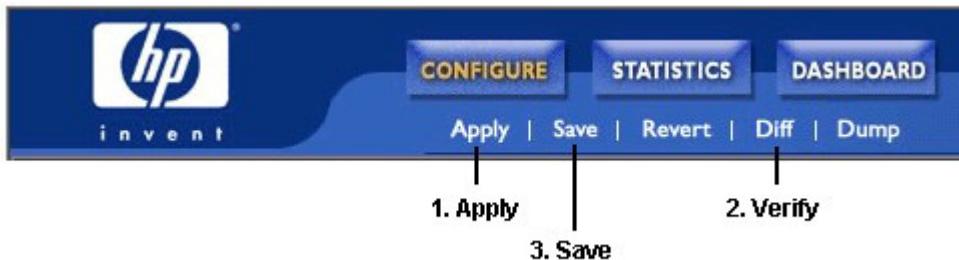
Port:1  
Port:17  
Port:18  
Port:19  
Port:22

Add>> <<Remove

Submit Delete

- Click **Submit**.

3. Apply, verify, and save the configuration. The external Layer 2 switches should also be configured for VLANs and tagging.



## FDB static entries

Static entries in the Forwarding Database (FDB) allow the switch to forward packets without flooding ports to perform a lookup. A FDB static entry is a MAC address associated with a specific port and VLAN. The GbE2 supports 128 static entries. Static entries are manually configured, using the /cfg/l2/fdb/static command.

FDB static entries are permanent, so the FDB Aging value does not apply to them. Static entries are manually added to the FDB, and manually deleted from the FDB.

Incoming frames that contain the static entry as the source MAC can use only ports configured for the static entry.

## Trunking support for FDB static entries

A FDB static entry can be added to a port that is a member of a trunk group, as follows:

- Static (manually configured) trunk group
- Dynamic (LACP) trunk group

The trunk group supports the FDB static entry. If the port with the static entry fails, other ports in the trunk handle the traffic. If the port is removed from the trunk, the static entry is removed from the trunk, but remains configured on the port.

The FDB information commands (/info/l2/fdb) display trunk support for static FDB entries, if applicable:

>> Forwarding Database# dump				
MAC address	VLAN	Port	Trnk	State
00:00:2e:9b:db:f8	1		1	TRK
00:00:5e:00:01:f4	1	24		FWD
00:01:81:2e:b5:60	1	24		FWD
00:02:a5:e9:76:30	1		1	TRK
00:03:4b:e2:15:f1	1	24		FWD

## Configuring a static FDB entry

Perform the following actions to configure a static FDB entry:

Main# /cfg/l2/fdb/static	(Select static FDB menu)
>> Static FDB# add 00:60:af:00:02:30	
Enter VLAN number: 2	
Enter port (1-24): 2	
>> Static FDB# apply	(Apply the configuration)
>> Static FDB# save	(Save the configuration)

# Spanning Tree Protocol

## Introduction

When multiple paths exist on a network, Spanning Tree Protocol (STP) configures the network so that a switch uses only the most efficient path. The following topics are discussed in this chapter:

- Overview
- Bridge Protocol Data Units (BPDUs)
- Spanning Tree Group (STG) configuration guidelines
- Multiple Spanning Trees

## Overview

Spanning Tree Protocol (STP) detects and eliminates logical loops in a bridged or switched network. STP forces redundant data paths into a standby (blocked) state. When multiple paths exist, STP configures the network so that a switch uses only the most efficient path. If that path fails, STP automatically sets up another active path on the network to sustain network operations.

The GbE2 Interconnect Switch supports IEEE 802.1d Spanning Tree Protocol for STG 1, and Per VLAN Spanning Tree Protocol (PVST+) for STGs 2-32, by default.



**NOTE:** The GbE2 Interconnect Switch also supports IEEE 802.1w Rapid Spanning Tree Protocol and IEEE 802.1s Multiple Spanning Tree Protocol. For more information, see the “RSTP and MSTP” chapter in this guide.

## Bridge Protocol Data Units

To create a spanning tree, the application switch generates a configuration Bridge Protocol Data Unit (BPDU), which it then forwards out of its ports. All switches in the Layer 2 network participating in the spanning tree gather information about other switches in the network through an exchange of BPDUs.

A BPDU is a 64-byte packet that is sent out at a configurable interval, which is typically set for two seconds. The BPDU is used to establish a path, much like a “hello” packet in IP routing. BPDUs contain information about the transmitting bridge and its ports, including bridge and MAC addresses, bridge priority, port priority, and port path cost. If the ports are tagged, each port sends out a special BPDU containing the tagged information.

The generic action of a switch on receiving a BPDU is to compare the received BPDU to its own BPDU that it will transmit. If the received BPDU has a priority value closer to zero than its own BPDU, it will replace its BPDU with the received BPDU. Then, the application switch adds its own bridge ID number and increments the path cost of the BPDU. The application switch uses this information to block any redundant paths.

## Determining the path for forwarding BPDUs

When determining which port to use for forwarding and which port to block, the GbE2 Interconnect Switch uses information in the BPDU, including each bridge priority ID. A technique based on the “lowest root cost” is then computed to determine the most efficient path for forwarding.

## Bridge priority

The bridge priority parameter controls which bridge on the network is the STP root bridge. To make one switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The bridge priority is configured using the `/cfg/12/stp/brg/prior` command in the CLI.

## Port priority

The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The port priority is configured using the `/cfg/12/stp/port x/prior` command in the CLI.

## Port path cost

The port path cost assigns lower values to high-bandwidth ports, such as Gigabit Ethernet, to encourage their use. The objective is to use the fastest links so that the route with the lowest cost is chosen. A value of 0 indicates that port cost is computed dynamically based on link speed. This works when forcing link speed, so it does not just apply to "auto negotiated link speed".

By default, all switch ports have the path cost set to 4, independent of the link speed. To use dynamic path cost, based on link speed, set the path cost to 0 (zero). For example, if the path cost is set to zero:

- A 100 Mbps link receives a path cost of 19
- A 10 Mbps link receives a path cost of 100

## Spanning Tree Group configuration guidelines

This section provides important information on configuring Spanning Tree Groups (STGs).

### Default Spanning Tree configuration

In the default configuration, a single STG with the ID of 1 includes all ports on the switch. It is called the default STG. All other STGs (except the default STG) are empty, and VLANs must be added by the user.

You cannot assign ports directly to an STG. Add the ports to a VLAN, and add the VLAN to the STG. All STGs are enabled by default and assigned an ID number from 1 to 32.

An STG cannot be deleted, only disabled. If you disable the STG while it still contains VLAN members, Spanning Tree will be off on all ports belonging to that VLAN.

### Adding a VLAN to a Spanning Tree Group

If no VLANs exist beyond the default VLAN 1, see the "Creating a VLAN" section in this chapter for information on adding ports to VLANs.

Add the VLAN to the STG using the `/cfg/l2/stp <stg number>/add <vlan number>` command.

### Creating a VLAN

When you create a VLAN, then that VLAN automatically belongs to STG 1, the default STG. If you want the VLAN in another STG, you must move the VLAN by assigning it to another STG.

To move a newly created VLAN to an existing STG:

1. Create the VLAN.
2. Add the VLAN to an existing STG.

When creating a VLAN also consider the following:

- A VLAN cannot belong to more than one STG.
- VLANs that span multiple switches must be mapped within the same Spanning Tree Group (have the same STG ID) across all the switches.

### Rules for VLAN tagged ports

Rules for VLAN tagged ports are listed below:

- If a port is tagged, it can belong to multiple STGs.
- Tagged ports can belong to more than one STG, but untagged ports can belong to only one STG.
- When a tagged port belongs to more than one STG, the egress BPDUs are tagged to distinguish the BPDUs of one STG from those of another STG.
- An untagged port cannot span multiple STGs.

## Adding and removing ports from STGs

Information on adding and removing ports from STGs is as follows:

- By default, all ports belong to VLAN 1 and STG 1.
- Each port is always a member of at least one VLAN. Each VLAN is always a member of at least one STG. Port membership within VLANs can be changed, and VLAN membership within STGs can be changed. To move a port from one STG to another, move the VLAN to which the port belongs, or move the port to a VLAN that belongs to the STG.
- When you remove a port from a VLAN, that port is also removed from the STG to which the VLAN belongs. However, if that port belongs to another VLAN in the same STG, the port remains in the STG.
- If you remove an untagged port from a non-default VLAN and STG, it is added to VLAN 1 and STG 1.

The relationship between ports, trunk groups, VLANs, and spanning trees is shown in the following table.

**Table 10** Ports, trunk groups, and VLANs

Switch element	Belongs to
Port	Trunk group, or One or more VLANs
Trunk group	One or more VLANs
VLAN (non-default)	One Spanning Tree Group

## Assigning cost to ports and trunk groups

When you configure a trunk group to participate in a Spanning Tree Group, manually assign port and trunk costs to ensure that each trunk group has a lower STP cost than the cost of each port within the trunk group. This ensures that the trunk group remains in the Forwarding state.

## Multiple Spanning Trees

Each GbE2 Interconnect Switch supports a maximum of 32 Spanning Tree Groups (STGs). Multiple STGs provide multiple data paths, which can be used for load-balancing and redundancy.

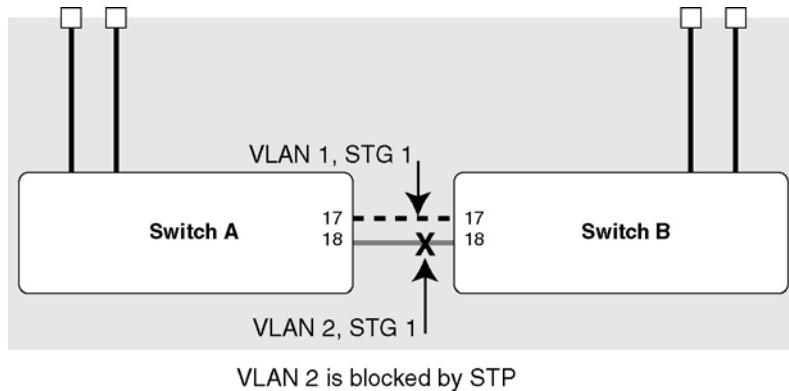
You enable independent links on two GbE2 Interconnect Switches using multiple STGs by configuring each path with a different VLAN and then assigning each VLAN to a separate STG. Each STG is independent. Each STG sends its own Bridge Protocol Data Units (BPDUs), and each STG must be independently configured.

The STG, or bridge group, forms a loop-free topology that includes one or more virtual LANs (VLANs). The switch supports 32 STGs running simultaneously. The default STG 1 supports IEEE 802.1d Spanning Tree Protocol, and may contain more than one VLAN. All other STGs support Per VLAN Spanning Tree (PVST+), and may contain only one VLAN each. The switch can support multiple VLANs in STGs 2-32; however, you must enable IEEE 802.1s Multiple Spanning Tree Protocol mode. For more information, see the “RSTP and MSTP” chapter in this guide.

## Why do we need Multiple Spanning Trees?

The following figure shows a simple example of why we need multiple Spanning Trees. This example assumes that port 17 and 18 are not part of Trunk Group 1. Two VLANs (VLAN 1 and VLAN 2) exist between Switch A and Switch B. If the same Spanning Tree Group is enabled on both switches, the switches see an apparent loop and block port 18 on Switch B, which cuts off communication between the switches for VLAN 2.

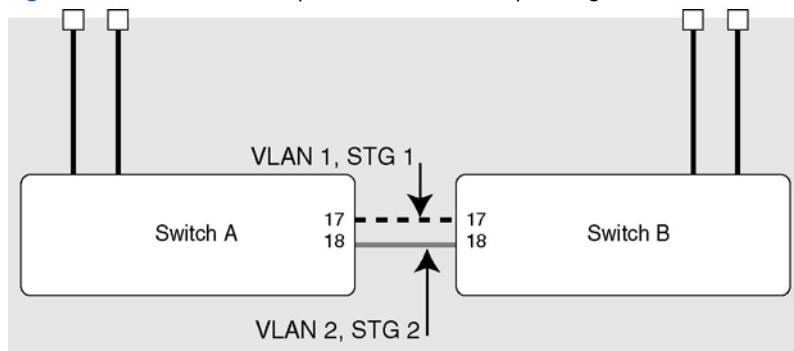
**Figure 9** Two VLANs on one instance of Spanning Tree Protocol



VLAN 2 is blocked by STP

In the following figure, VLAN 1 and VLAN 2 belong to different Spanning Tree Groups. The two instances of spanning tree separate the topology without forming a loop, so that both VLANs can forward packets between the switches without losing connectivity.

**Figure 10** Two VLANs on separate instances of Spanning Tree Protocol



Spanning Tree Group 1: VLAN 1

Spanning Tree Group 2: VLAN 2

## VLAN participation in Spanning Tree Groups

The following table shows which switch ports participate in each Spanning Tree Group. By default, server ports (ports 1-16) do not participate in Spanning Tree, even though they are members of their respective VLANs.

**Table 11** VLAN participation in Spanning Tree Groups

	VLAN 1	VLAN 2
Switch A	Spanning Tree Group 1 Port 17	Spanning Tree Group 2 Port 18
Switch B	Spanning Tree Group 1 Port 17	Spanning Tree Group 2 Port 18

## Configuring Multiple Spanning Tree Groups

This section explains how to assign each VLAN to its own Spanning Tree Group on the HP ProLiant BL p-Class GbE2 Interconnect Switches A and B.

By default, Spanning Tree Groups 2-32 are empty, and Spanning Tree Group 1 contains all configured VLANs until individual VLANs are explicitly assigned to other Spanning Tree Groups. Except for the default Spanning Tree Group 1, which may contain more than one VLAN, Spanning Tree Groups 2-32 may contain only one VLAN each.



**NOTE:** Each instance of Spanning Tree Group is enabled by default.

## Configuring Switch A (CLI example)

1. Configure port and VLAN membership on Switch A as described in the “Configuring Ports and VLANs on Switch A (CLI example)” section, in the “VLANs” chapter of this guide.
2. Add VLAN 2 to Spanning Tree Group 2.

```
>> /cfg/l2/stp 2                                (Select Spanning Tree Group 2)
>> Spanning Tree Group 2# add 2                (Add VLAN 2)
```

VLAN 2 is automatically removed from spanning tree group 1.

3. Apply and save.

```
>> apply                                         (Apply the port configurations)
>> save                                          (Save the port configurations)
```

## Configuring Switch B (CLI example)

1. Configure port and VLAN membership as described in the “Configuring Ports and VLANs on Switch B (CLI example)” section in the “VLANs” chapter of this guide.
2. Add VLAN 2 to Spanning Tree Group 2.

```
>> /cfg/l2/stp 2                                (Select Spanning Tree Group 2)
>> Spanning Tree Group 2# add 2                (Add VLAN 2)
```

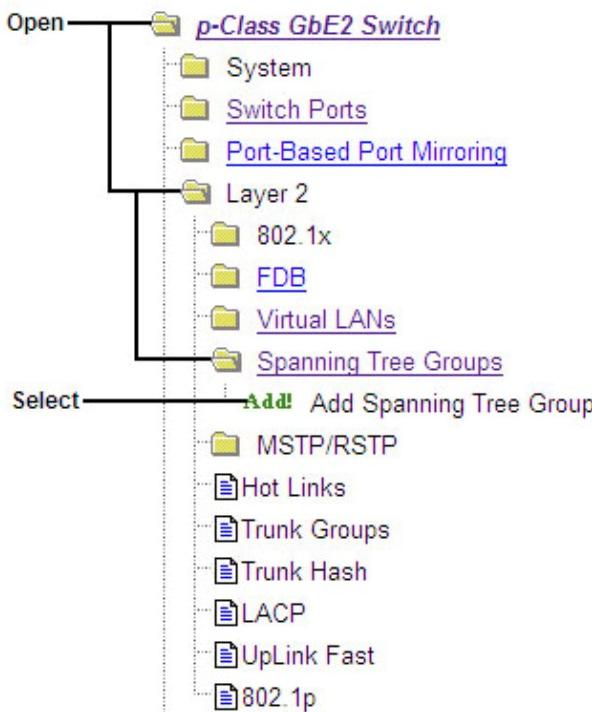
3. VLAN 2 is automatically removed from Spanning Tree Group 1.

4. Apply and save.

```
>> apply                                         (Apply the port configurations)
>> save                                           (Save the port configurations)
```

## Configuring Switch A (BBI example)

1. Configure port and VLAN membership on Switch A as described in the “Configuring Ports and VLANs on Switch A (BBI example)” section, in the “VLANs” chapter of this guide.
2. Add VLAN 2 to Spanning Tree Group 2.
  - a. Click the **Configure** context button on the Toolbar.
  - b. Open the Spanning Tree Groups folder, and select **Add Spanning Tree Group**.



- c. Enter the Spanning Tree Group number and set the Switch Spanning Tree State to on. To add a VLAN to the Spanning Tree Group, select the VLAN in the VLANs Available list, and click **Add**. VLAN 2 is automatically removed from Spanning Tree Group 1.

**Switch Spanning Tree Group Configuration**

Spanning Tree Group ID (1-32)	2
Switch Spanning Tree State	on
Bridge Priority (0-65535)	32768
Bridge Hello Time (1-10secs)	2
Bridge Max Age (6-40secs)	20
Bridge Forward Delay (4-30secs)	15

VLANs Available
VLANs in STG

Vlan ID:Name  
 20:ConnectVLAN  
 100:UplinkVLAN  
 134:VLAN 134

**Add>>**  
**<<Remove**

Vlan ID:Name  
 1:Default VLAN

**Switch Spanning Tree Port Configuration**

Switch Port	Port Priority	Port Path Cost	Port Spanning Tree State
1	128	4	on
2	128	4	on

- d. Scroll down, and click **Submit**.  
 3. Apply, verify, and save the configuration.



## Port Fast Forwarding

Port Fast Forwarding permits a port that participates in Spanning Tree to bypass the Listening and Learning states and enter directly into the Forwarding state. While in the Forwarding state, the port listens to the BPDUs to learn if there is a loop and, if dictated by normal STG behavior (following priorities, etc.), the port transitions into the Blocking state.

This feature permits the GbE2 Interconnect Switch to interoperate well within Rapid Spanning Tree (RSTP) networks.

## Configuring Port Fast Forwarding

Use the following CLI commands to enable Port Fast Forwarding on an external port.

```
>> # /cfg/l2/stp 1/port 19          (Select port 19)
>> Spanning Tree Port 19# fastfwd ena (Enable Port Fast Forwarding)
>> Spanning Tree Port 19# apply      (Make your changes active)
>> Spanning Tree Port 19# save      (Save for restore after reboot)
```

## Fast Uplink Convergence

Fast Uplink Convergence enables the GbE2 to quickly recover from the failure of the primary link or trunk group in a Layer 2 network using Spanning Tree Protocol. Normal recovery can take as long as 60 seconds, while the backup link transitions from Blocking to Listening to Learning and then Forwarding states. With Fast Uplink Convergence enabled, the GbE2 immediately places the secondary path into Forwarding state, and sends multicasts of addresses in the forwarding database (FDB) and ARP table over the secondary link so that upstream switches can learn the new path.

### Configuration guidelines

When you enable Fast Uplink Convergence, GbE2 software automatically makes the following configuration changes:

- Increases the bridge priority to 65500 so that it does not become the root switch.
- Increases the cost of all of the external ports by 3000, across all VLANs and Spanning Tree Groups. This ensures that traffic never flows through the GbE2 to get to another switch unless there is no other path.

When you disable Fast Uplink Convergence, the bridge priorities and path cost are set to their default values for all STP groups.

## Configuring Fast Uplink Convergence

Use the following CLI commands to enable Fast Uplink Convergence on external ports:

```
>> # /cfg/l2/upfast ena    (Enable Fast Uplink convergence)
>> Layer 2# apply          (Make your changes active)
>> Layer 2# save            (Save for restore after reboot)
```

## Hot Links

For network topologies that require Spanning Tree to be turned off, Hot Links provides basic link redundancy with fast recovery.

Hot Links consists of up to three triggers. A trigger consists of a pair of layer 2 interfaces, each containing either an individual port or trunk. One interface is the Master, and the other is a Backup. While the Master interface is set to the active state and forwards traffic, the Backup interface is set to the standby state and blocks traffic until the Master interface fails. If the Master interface fails, the Backup interface is set to active and forwards traffic. Once the Master interface is restored, it transitions to the standby state and blocks traffic until the Backup interface fails.

You may select either a physical port or a static trunk as a Hot Link interface. Only cross-connect ports (17-18) and external ports (19-24) can be members of a Hot Links trigger interface.

## Forward Delay

The Forward Delay timer allows Hot Links to monitor the Master and Backup interfaces for link stability before selecting one interface to transition to the active state. Before the transition occurs, the interface must maintain a stable link for the duration of the Forward Delay interval.

For example, if you set the Forward delay timer to 10 seconds (`/cfg/l2/hotlink/trigger x/fdelay 10`), the switch will select an interface to become active only if a link remained stable for the duration of the Forward Delay period. If the link is unstable, the Forward Delay period starts again.

## Pre-emption

You can configure the Master interface to resume the active state whenever it becomes available. With Hot Links pre-emption enabled (`/cfg/l2/hotlink/trigger x/preempt ena`), the Master interface transitions to the active state immediately upon recovery. The Backup interface immediately transitions to the standby state. If Forward Delay is enabled, the transition occurs when an interface has maintained link stability for the duration of the Forward Delay period.

## FDB Update

Use the FDB update option to notify other devices on the network about updates to the Forwarding Database (FDB). When you enable FDB update (`/cfg/l2/hotlinks/trigger x/sndfdb ena`), the GbE2 sends multicasts of addresses in the forwarding database (FDB) over the active interface, so that other devices on the network can learn the new path.

The Hot Links FBD update option uses the station update rate (`/cfg/l2/update`) to determine the rate at which to send FDB packets.

## Configuration Guidelines

The following configuration guidelines apply to Hot links:

- Only external ports and inter-switch links can be configured as Hot Links.
- Ports that are configured as Hot Link interfaces must have STP disabled.
- When Hot Links is turned on, MSTP must be disabled.
- When Hot Links is turned on, UplinkFast (`/cfg/l2/upfast`) must be turned off (`/cfg/l2/mrst/off`).
- A port that is a member of the Master interface cannot be a member of the Backup interface. A port that is a member of one Hot Links trigger cannot be a member of another Hot Links trigger.
- An individual port that is configured as a Hot Link interface cannot be a member of a trunk.
- An LACP trunk cannot be configured as a Hot Link interface.

## Configuring Hot Links

Use the following CLI commands to configure Hot Links:

```
>> # /cfg/l2/hotlink/trigger 1 ena
>> Trigger 1# master/port 20
>> Master# ..
>> Trigger 1# backup/port 21
>> Backup# ..
>> Trigger 1# ..
>> Hot Links# on
```

# RSTP and MSTP

## Introduction

Rapid Spanning Tree Protocol (IEEE 802.1w) enhances the Spanning Tree Protocol (IEEE 802.1d) to provide rapid convergence on Spanning Tree Group 1. Multiple Spanning Tree Protocol (IEEE 802.1s) extends the Rapid Spanning Tree Protocol to provide both rapid convergence and load balancing in a VLAN environment.

The following topics are discussed in this chapter:

- Rapid Spanning Tree Protocol (RSTP)
- Multiple Spanning Tree Protocol (MSTP)

## Rapid Spanning Tree Protocol

Rapid Spanning Tree Protocol (RSTP) provides rapid convergence of the spanning tree and provides for fast reconfiguration critical for networks carrying delay-sensitive traffic such as voice and video. RSTP significantly reduces the time to reconfigure the active topology of the network when changes occur to the physical topology or its configuration parameters. RSTP reduces the bridged-LAN topology to a single Spanning Tree.

For more information about Spanning Tree Protocol, see the “Spanning Tree Protocol” chapter in this guide.

RSTP parameters are configured in Spanning Tree Group 1. STP Groups 2-32 do not apply to RSTP, and must be cleared. There are new STP parameters to support RSTP, and some values to existing parameters are different.

RSTP is compatible with devices that run 802.1d Spanning Tree Protocol. If the switch detects 802.1d BPDUs, it responds with 802.1d-compatible data units. RSTP is not compatible with Per VLAN Spanning Tree (PVST) protocol.

## Port state changes

The port state controls the forwarding and learning processes of Spanning Tree. In RSTP, the port state has been consolidated to the following: discarding, learning, and forwarding.

**Table 12** RSTP vs. STP port states

Operational status	STP port state	RSTP port state
Enabled	Blocking	Discarding
Enabled	Listening	Discarding
Enabled	Learning	Learning
Enabled	Forwarding	Forwarding
Disabled	Disabled	Discarding

## Port type and link type

Spanning Tree Configuration includes the following parameters to support RSTP and MSTP:

- Edge port
- Link type

Although these parameters are configured for Spanning Tree Groups 1-32 (/cfg/12/stp x/port x), they only take effect when RSTP/MSTP is turned on.

## Edge port

A port that connects to a server or stub network is called an edge port. Therefore, ports 1-16 should have **edge** enabled. Edge ports can start forwarding as soon as the link is up.

Edge ports do not take part in Spanning Tree, and should not receive BPDUs. If a port with **edge** enabled does receive a BPDU, it begins STP processing until it is re-enabled.

## Link type

The link type determines how the port behaves in regard to Rapid Spanning Tree. The link type corresponds to the duplex mode of the port. A full-duplex link is point-to-point (**p2p**), while a half-duplex link should be configured as **shared**. If you select **auto** as the link type, the port dynamically configures the link type.

## RSTP configuration guidelines

This section provides important information about configuring Rapid Spanning Tree Groups:

- When RSTP is turned on, STP parameters apply only to STP Group 1.
- Before RSTP is turned on, STP Groups 2-32 must be disabled and cleared.

## RSTP configuration example

This section provides steps to configure Rapid Spanning Tree on the HP ProLiant BL p-Class GbE2 Interconnect Switch, using the Command-Line Interface (CLI) or the Browser-Based Interface (BBI).

### Configuring Rapid Spanning Tree (CLI example)

1. Configure port and VLAN membership on the switch, as described in the “Configuring Ports and VLANs (CLI example)” section in the “VLANs” chapter of this guide.
2. Disable and clear STP groups 2 through 32.

```
>> /cfg/l2/stp 2          (Select Spanning Tree Group 2)
>> Spanning Tree Group 2# clear (Clear STP Group 2 parameters)
>> Spanning Tree Group 2# off   (Turn off STP Group 2)
```

3. Set the Spanning Tree mode to Rapid Spanning Tree.

```
>> /cfg/l2/mrst           (Select Multiple Spanning Tree menu)
>> Multiple Spanning Tree# mode rstp   (Set mode to Rapid Spanning Tree)
>> Multiple Spanning Tree# on           (Turn Rapid Spanning Tree on)
```

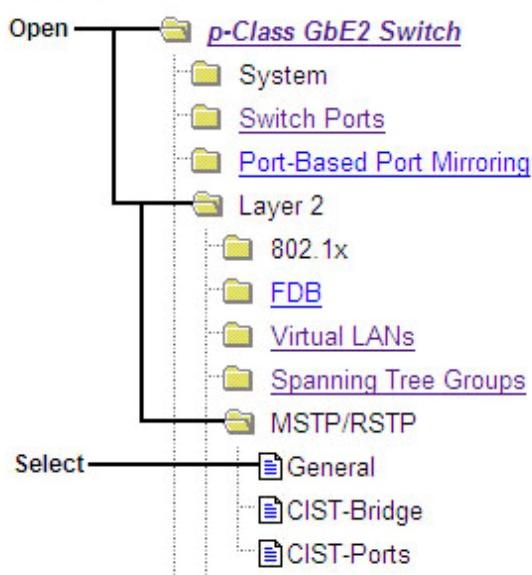
4. Configure STP Group 1 parameters.

```
>> /cfg/l2/stp 1          (Select Spanning Tree Protocol menu)
>> Spanning Tree Group 1# add 2      (Add VLAN 2 STP group 1)
>> Spanning Tree Group 1# apply       (Apply the configurations)
```

### Configuring Rapid Spanning Tree Protocol (BBI example)

1. Configure port and VLAN membership on HP ProLiant BL p-Class GbE2 Interconnect Switch A, as described in the “Configuring Ports and VLANs (BBI example)” section in the “VLANs” chapter of this guide.
2. Disable and clear STP groups 2 through 32.

3. Configure RSTP general parameters.
  - a. Click the **Configure** context button on the Toolbar.
  - b. Open the MSTP/RSTP folder, and select **General**.



- c. Select RSTP mode, and set the MSTP/RSTP state to **ON**.

MSTP/RSTP General Configuration	
Region Name	TestBed
Revision Level (0-65535)	0
Max. Hop Count (4-60)	20
MSTP/RSTP Mode	RSTP
MSTP/RSTP State	ON

- d. Click **Submit**.
4. Apply, verify, and save the configuration.



# Multiple Spanning Tree Protocol

IEEE 802.1s Multiple Spanning Tree extends the IEEE 802.1w Rapid Spanning Tree Protocol through multiple Spanning Tree Groups. MSTP maintains up to 32 spanning-tree instances that correspond to STP Groups 1-32.

In Multiple Spanning Tree Protocol (MSTP), several VLANs can be mapped to each Spanning-Tree instance. Each Spanning-Tree instance is independent of other instances. MSTP allows frames assigned to different VLANs to follow separate paths, each path based on an independent Spanning-Tree instance. This approach provides multiple forwarding paths for data traffic, enabling load balancing, and reducing the number of Spanning-Tree instances required to support a large number of VLANs.

## MSTP region

A group of interconnected bridges that share the same attributes is called an MST region. Each bridge within the region must share the following attributes:

- Alphanumeric name
- Version number
- VLAN-to-STG mapping scheme

MSTP provides rapid reconfiguration, scalability, and control due to the support of regions, and multiple Spanning-Tree instances support within each region.

## Common Internal Spanning Tree

The Common Internal Spanning Tree (CIST) provides a common form of Spanning Tree Protocol, with one Spanning Tree instance that can be used throughout the MSTP region. CIST allows the switch to interoperate with legacy equipment, including devices that run IEEE 802.1d (STP).

CIST allows the MSTP region to act as a virtual bridge to other bridges outside of the region, and provides a single Spanning-Tree instance to interact with them.

CIST port configuration includes Hello time, Edge port status (enable/disable), and Link Type. These parameters do not affect Spanning Tree Groups 1-32. They apply only when the CIST is used.

## MSTP configuration guidelines

This section provides important information about configuring Multiple Spanning Tree Groups:

- When you turn on MSTP, the switch automatically moves all VLANs from STP Group 1 to the Common Internal Spanning Tree (CIST).
- Region Name and version number must be configured. Each bridge in the region must have the same name and version number.
- The VLAN and STP Group mapping must be the same across all bridges in the region.

## MSTP configuration example

This section provides steps to configure Multiple Spanning Tree Protocol on the HP ProLiant BL p-Class GbE2 Interconnect Switch, using the Command-Line Interface (CLI) or the Browser-Based Interface (BBI).

## Configuring Multiple Spanning Tree Protocol (CLI example)

1. Configure port and VLAN membership on the switch, as described in the “Configuring Ports and VLANs (CLI example)” section in the “VLANs” chapter of this guide.
2. Set the mode to Multiple Spanning Tree, and configure MSTP region parameters.

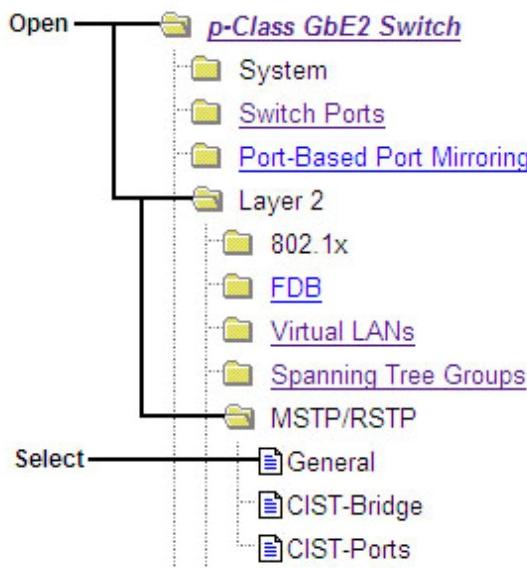
```
>> /cfg/12/ mrst                                (Select Multiple Spanning Tree menu)
>> Multiple Spanning Tree# mode mstp    (Set mode to
                                         Multiple Spanning Trees)
>> Multiple Spanning Tree# on           (Turn Multiple Spanning Trees on)
>> Multiple Spanning Tree# name xxxxxxxx (Define the Region name)
>> Multiple Spanning Tree: version xx (Define the Region version number)
```

3. Assign VLANs to Spanning Tree Groups.

```
>> /cfg/12/stp 2                                (Select Spanning Tree Group 2)
>> Spanning Tree Group 2# add 2                (Add VLAN 2)
>> Spanning Tree Group 2# apply                 (Apply the configurations)
```

## Configuring Multiple Spanning Tree Protocol (BBI example)

1. Configure port and VLAN membership on the switch, as described in the “Configuring Ports and VLANs (BBI example)” section in the “VLANs” chapter of this guide.
2. Configure MSTP general parameters.
  - a. Click the **Configure** context button on the Toolbar.
  - b. Open the MSTP/RSTP folder, and select **General**.



- c. Enter the region name and revision level. Select MSTP mode, and set the MSTP/RSTP state to **ON**.

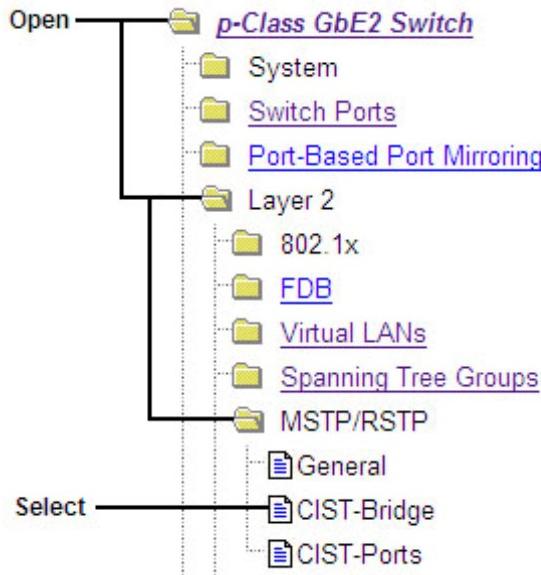
**MSTP/RSTP General Configuration**

Region Name	TestBed
Revision Level (0-65535)	0
Max. Hop Count (4-60)	20
MSTP/RSTP Mode	MSTP
MSTP/RSTP State	ON

**Submit**    **Default CIST**

- d. Click **Submit**.

3. Configure Common Internal Spanning Trees (CIST) bridge parameters.
- a. Open the MSTP/RSTP folder, and select **CIST-Bridge**.



- b. Change the Bridge Priority, Maximum Age, and Forward Delay values, if necessary.

### Common Internal Spanning Tree Bridge Configuration

Bridge Priority (0-65535)	32768
Max. Age (6-40 secs)	20
Forward Delay (4-30 secs)	15

**VLANs Available**

**Add>>**

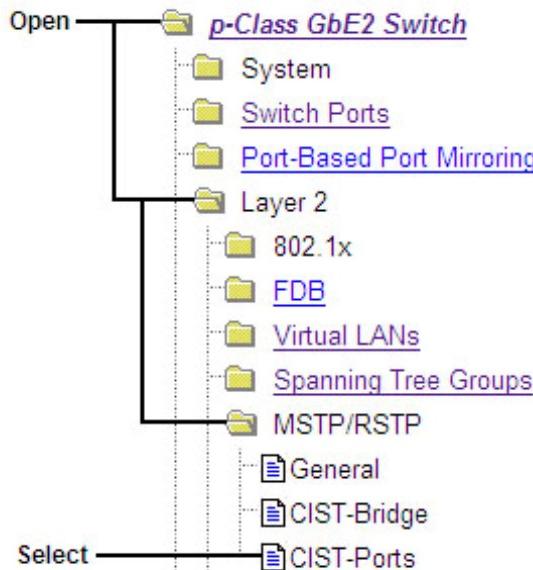
**Cist VLANs**

Vlan ID:Name  
1:Default VLAN

**Submit**

c. Click **Submit**.

4. Configure Common Internal Spanning Tree (CIST) port parameters.
- a. Open the MSTP/RSTP folder, and select **CIST-Ports**.



- b. Click a port number to select it.

Ports Common Internal Spanning Tree Configuration						
	CIST Port	Priority	Port Path Cost	Link Type	Edge Port State	Port STP State
Select →	<u>1</u>	128	20000	auto	enabled	ON
	<u>2</u>	128	20000	auto	enabled	ON
	<u>3</u>	128	20000	auto	enabled	ON
	<u>4</u>	128	20000	auto	enabled	ON
	<u>5</u>	128	20000	auto	enabled	ON
	<u>6</u>	128	20000	auto	enabled	ON
	<u>7</u>	128	20000	auto	enabled	ON
	<u>8</u>	128	20000	auto	enabled	ON
	<u>9</u>	128	20000	auto	enabled	ON
	<u>10</u>	128	20000	auto	enabled	ON
	<u>11</u>	128	20000	auto	enabled	ON

- c. Enter the Port Priority, Path Cost, and select the Link Type. Set the CIST Port State to ON.

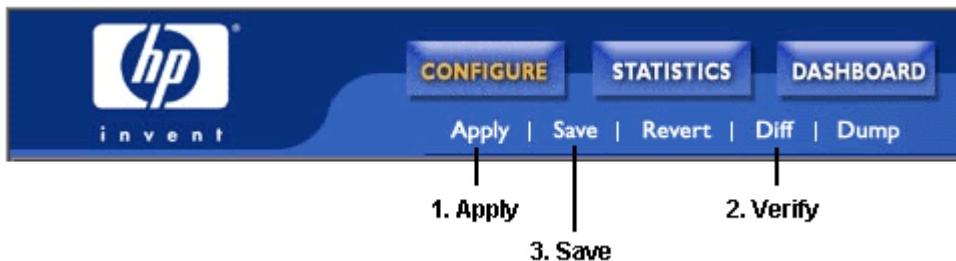
### Common Internal Spanning Tree Port 1 Configuration

Port Priority (0-240)	128
Path Cost (1-200000000, 0 for auto)	20000
Link Type	Auto
Enable/Disable Edge	Enabled
Port STP State	ON
Hello Time (1-10 secs)	2

Submit

- d. Click Submit.

5. Apply, verify, and save the configuration.



# Quality of Service

## Introduction

Quality of Service features allow you to allocate network resources to mission-critical applications at the expense of applications that are less sensitive to such factors as time delays or network congestion. You can configure your network to prioritize specific types of traffic, ensuring that each type receives the appropriate Quality of Service (QoS) level.

The following topics are discussed in this section:

- Quality of Service Overview
- Using ACL Filters
- Using DSCP Values to Provide QoS
- Using 802.1p Priorities to Provide QoS
- Queuing and Scheduling

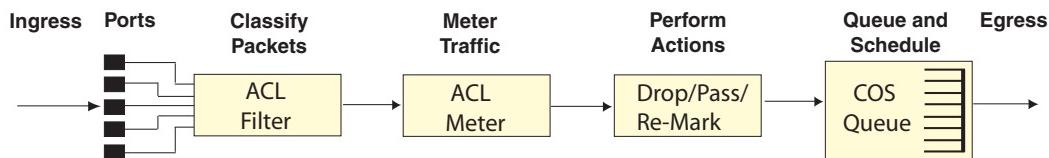
## Overview

QoS helps you allocate guaranteed bandwidth to the critical applications, and limit bandwidth for less critical applications. Applications such as video and voice must have a certain amount of bandwidth to work correctly; using QoS, you can provide that bandwidth when necessary. Traffic for applications that are sensitive to timing out or cannot tolerate delay can be assigned to a high-priority queue.

By assigning QoS levels to traffic flows on your network, you can ensure that network resources are allocated where they are needed most. QoS features allow you to prioritize network traffic, thereby providing better service for selected applications.

The following figure shows the basic QoS model used by the GbE2.

**Figure 11** QoS model



The GbE2 uses the Differentiated Services (DiffServ) architecture to provide QoS functions. DiffServ is described in IETF RFCs 2474 and 2475.

With DiffServ, you can establish policies to direct traffic. A policy is a traffic-controlling mechanism that monitors the characteristics of the traffic, (for example, its source, destination, and protocol) and performs a controlling action on the traffic when certain characteristics are matched.

The GbE2 can classify traffic by reading the IEEE 802.1p priority value, or by using filters to match specific criteria. When network traffic attributes match those specified in a traffic pattern, the policy instructs the GbE2 to perform specified actions on each packet that passes through it. The packets are assigned to different Class of Service (COS) queues and scheduled for transmission.

The basic GbE2 QoS model works as follows:

- Classify traffic:
  - Read DSCP
  - Read 802.1p Priority
  - Match ACL filter parameters
- Meter traffic:
  - Define bandwidth and burst parameters
  - Select actions to perform on in-profile and out-of-profile traffic

- Perform actions:
  - Drop packets
  - Pass packets
  - Mark DSCP or 802.1p Priority
  - Set COS queue (with or without re-marking)
- Queue and schedule traffic:
  - Place packets in one of eight COS queues
  - Schedule transmission based on the COS queue weight

## Using ACL filters

Access Control Lists are filters that allow you to classify and segment traffic, so you can provide different levels of service to different traffic types. Each filter defines the conditions that must match for inclusion in the filter, and also the actions that are performed when a match is made.

## Summary of packet classifiers

The GbE2 allows you to classify packets based on various parameters, such as:

- Ethernet
  - Source MAC address
  - Destination MAC address
  - VLAN number/mask
  - Ethernet type
  - Ethernet Priority, which is the IEEE 802.1p Priority
- IPv4
  - Source IP address/mask
  - Destination IP address/mask
  - Type of Service value
  - IP protocol number: The protocol number or name as shown in the following table:

**Table 13** Well-known protocol types

Number	Protocol name
1	icmp
2	igmp
6	tcp
17	udp
89	ospf
112	vrrp

- TCP/UDP
  - TCP/UDP application source port, as shown in the table titled “Well-Known Application Ports”
  - TCP/UDP application destination port, as shown in the table titled “Well-Known Application Ports”
  - TCP/UDP flag value, as shown in the table titled “Well-Known TCP Flag Values”

**Table 14** Well-known application ports

Number	TCP/UDP Application	Number	TCP/UDP Application	Number	TCP/UDP Application
20	ftp-data	79	Finger	179	irc
21	ftp	80	http	194	imap3
22	ssh	109	pop2	220	ldap
23	telnet	110	pop3	389	https
25	smtp	111	sunrpc	443	rip

**Table 14** Well-known application ports

Number	TCP/UDP Application	Number	TCP/UDP Application	Number	TCP/UDP Application
37	time	119	nntp	520	rtsp
42	name	123	ntp	554	Radius
43	whois	143	imap	1645, 1812	Radius Accounting
53	domain	144	news	1813	hsrp
69	tftp	161	snmp	1985	
70	gopher	162	snmptrap		

**Table 15** Well-known TCP flag values

Flag	Value
URG	0x0020
ACK	0x0010
PSH	0x0008
RST	0x0004
SYN	0x0002
FIN	0x0001

- Packet Format
  - Ethernet format (eth2, 802.3)
  - Ethernet tagging format
- Egress port packets

## Summary of ACL actions

Actions determine how the traffic is treated. The GbE2 QoS actions include the following:

- Pass or Drop
- Re-mark a new DiffServ Code Point (DSCP)
- Re-mark the 802.1p field
- Set the COS queue

## Using ACL Blocks and ACL Groups

Access Control Lists (ACLs) allow you to classify packets according to a particular content in the packet header, such as the source address, destination address, source port number, destination port number, and others. Packet classifiers identify flows for more processing.

You can define a traffic profile by compiling a number of ACLs into an ACL Group, and assigning the ACL Group to a port. Each port can accept up to 96 filters, including ACL Groups.

Each ACL (or ACL Block) in an ACL Group has a precedence level, based on its position in the ACL Group. The first ACL added to the ACL Group has the highest precedence; the last ACL added has the lowest precedence (top to bottom). If a packet matches the highest precedence ACL, the following ACLs are also considered, in order of precedence.

ACL Groups are assigned and enabled on a per-port basis. Each ACL can be used by itself or in combination with other ACLs, ACL Blocks, or ACL Groups on a given switch port. When multiple ACLs are grouped together on a port, each ACL's position determines its order of precedence: the first or topmost ACL is checked first. When traffic is encountered at the switch port, if the ACL criteria match, its configured action takes place. Other ACLs are checked in order of precedence.

ACLs can be grouped in the following manner:

- **Access Control Lists**

Access Control Lists (ACLs) allow you to classify packets according to a particular content in the packet header, such as the source address, destination address, source port number, destination port number, and others. Packet classifiers identify flows for more processing.

The GbE2 supports up to 4096 ACLs. Each ACL defines one filter rule. Each filter rule is a collection of matching criteria, and can include an action (permit or deny the packet). For example:

<b>ACL 1:</b> VLAN = 1 SIP = 10.10.10.1 (255.255.255.0) Action = permit
--

- **Access Control Blocks**

An Access Control Block (ACL Block) is a collection of ACLs that define filtering criteria on the same set of fields and within the same mask. Each ACL in an ACL Block must match the same parameters and the same mask, range, and packet format type. For example:

ACL Block 1	
<b>ACL 1:</b> VLAN = 1 SIP = 10.10.10.1 (255.255.255.0) Action = permit	<b>ACL 2:</b> VLAN = 2 SIP = 10.10.10.2 (255.255.255.0) Action = deny
ACL Block 2	
<b>ACL 3:</b> PRI = 0 SIP = 20.20.20.1 (255.255.0.0) Action = deny	<b>ACL 4:</b> PRI = 1 DIP = 20.20.20.2 (255.255.0.0) Action = deny

All ACLs within an ACL Block remain at the same precedence level. Use ACL Blocks to define a number of ACLs that do not require different precedence levels, and therefore utilize only one of the eight available precedence levels. The GbE2 supports up to 4096 ACL Blocks.

- **Access Control Groups**

An Access Control Group (ACL Group) is a collection of ACLs and ACL Blocks. For example:

ACL Group 1	
ACLBLK 1	
<b>ACL 1:</b> VLAN = 1 SIP = 10.10.10.1 (255.255.255.0) Action = permit	<b>ACL 2:</b> VLAN = 2 SIP = 10.10.10.2 (255.255.255.0) Action = deny
<b>ACL 3:</b> PRI = 0 SIP = 20.20.20.1 (255.255.0.0) Action = deny	

In the example above, ACLBLK 1 can contain several ACLs, with each ACL defining a filter rule. ACLBLK 1 has a higher precedence than ACL 3, based on its position in the ACL Group.

Use ACL Groups to create a traffic profile by gathering ACLs and ACL Blocks into an ACL Group, and assigning the ACL Group to a port. The GbE2 Interconnect Switch supports up to 4096 ACL Groups.

## Port-Based QoS actions

You can define a profile for the aggregate traffic flowing through the GbE2, by assigning an ACL Group to the port and configuring a QoS meter (if desired). When you add ACL Groups to a port, make sure they are ordered correctly in terms of precedence.

For example, consider two ACL Groups, ACL Group 1 and ACL Group 2. Each contains three levels of precedence. If you add ACL Group 1 to a port, then add ACL Group 2 to the port, the port's ACL filters contain a total of six precedence levels. ACL Group 1 has precedence over ACL Group 2.

Each port supports up to seven precedence levels.

Actions taken by an ACL are called *In-Profile* actions. You can configure additional In-Profile and Out-of-Profile actions on a port. Data traffic can be metered, and re-marked to ensure that the traffic flow provides certain levels of service in terms of bandwidth for different types of network traffic.

## Metering

QoS metering provides different levels of service to data streams through user-configurable parameters. A meter is used to measure the traffic stream against a traffic profile, which you create. Thus, creating meters yields In-Profile and Out-of-Profile traffic, as follows:

**In-Profile**—If there is no meter configured or if the packet conforms to the meter, the packet is classified as In-Profile.

**Out-of-Profile**—If a meter is configured and the packet does not conform to the meter (exceeds the committed rate or maximum burst rate of the meter), the packet is classified as Out-of-Profile.

Using meters, you set a Committed Rate in Kb/s (1024 bits per second in each Kb/s). All traffic within this Committed Rate is In-Profile. Additionally, you set a Maximum Burst Size that specifies an allowed data burst larger than the Committed Rate for a brief period. These parameters define the In-Profile traffic.

Meters keep the sorted packets within certain parameters. You can assign an ACL to a meter, or perform actions on metered traffic, such as packet re-marking. Each port can accept up to 63 meters.

## Re-marking

Re-marking allows for the treatment of packets to be reset based on new network specifications or desired levels of service. You can configure the ACL to re-mark a packet as follows:

- Change the DSCP value of a packet, used to specify the service level traffic should receive.
- Change the 802.1p priority of a packet.

## Viewing ACL statistics

ACL statistics display how many packets hit (matched) each ACL. Use ACL statistics to check filter performance, and debug the ACL filters.

You must enable statistics (`cfg/acl/acl x/stats ena`) for each ACL that you want to monitor.

# ACL configuration examples

## Configure Access Control Lists (CLI example)

The following configuration examples illustrate how to use Access Control Lists (ACLs) to block traffic. These basic configurations illustrate common principles of ACL filtering.



**NOTE:** Each ACL filters traffic that ingresses on the port to which the ACL is added. The egrport classifier filters traffic that ingresses the port to which the ACL is added, and then egresses the port specified by egrport. In most common configurations, egrport is not used.

**Example 1:** Use this configuration to block traffic to a specific host.

```
>> Main# /cfg/acl/acl 1                                     (Define ACL 1)
>> ACL 1# ipv4/dip 100.10.1.116 255.255.255.255
>> Filtering IPv4# ..
>> ACL 1# action deny
>> ACL 1# /cfg/port 19/aclqos
>> Port 19 ACL# add acl 1
>> Port 19 ACL# apply
>> Port 19 ACL# save                                         (Add ACL to port 19)
```

In this example, all traffic that ingresses on port 19 is denied if it is destined for the host at IP address 100.10.1.116.

**Example 2:** Use this configuration to block traffic from a network destined for a specific host address.

```
>> Main# /cfg/acl/acl 1                                     (Define ACL 1)
>> ACL 1# ipv4/sip 100.10.1.0 255.255.255.0
>> ACL 1# ipv4/dip 200.20.1.116 255.255.255.255
>> Filtering IPv4# ..
>> ACL 1# action deny
>> ACL 1# /cfg/port 19/aclqos
>> Port 19 ACL# add acl 1
>> Port 19 ACL# apply
>> Port 19 ACL# save                                         (Add ACL to port 19)
```

In this example, all traffic that ingresses on port 19 with source IP from the class 100.10.1.0/24 and destination IP 200.20.1.116 is denied.

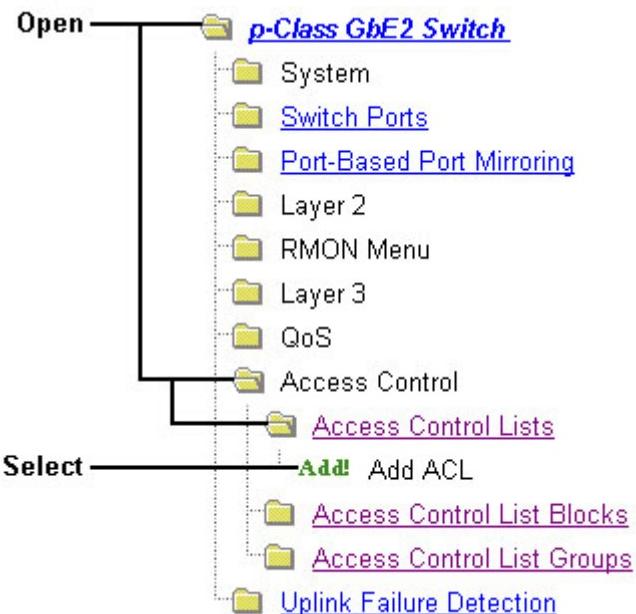
**Example 3:** Use this configuration to block all traffic from a network that is destined for a specific egress port.

```
>> Main# /cfg/acl/acl 1                                     (Define ACL 1)
>> ACL 1# ipv4/sip 100.10.1.0 255.255.255.0
>> Filtering IPv4# ..
>> ACL 1# egrport 3
>> ACL 1# action deny
>> ACL 1# /cfg/port 19/aclqos
>> Port 19 ACL# add acl 1
>> Port 19 ACL# apply
>> Port 19 ACL# save                                         (Add ACL to port 19)
```

In this example, all traffic that ingresses on port 19 from the network 100.10.1.0/24 and is destined for port 3 is denied.

## Configure Access Control Lists and Groups (BBI example 1)

1. Configure Access Control Lists (ACLs).
  - a. Click the **Configure** context button on the Toolbar.
  - b. Open the Access Control Lists folder, and select **Add ACL**.



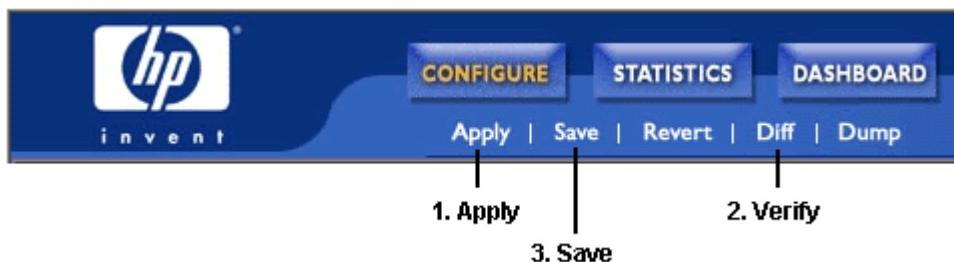
- c. Configure the ACL parameters. Set the Filter Action to **Deny**, the Ethernet Type to **IPv4**, and the Destination IP Address to **100.10.1.116**.

**Access Control List**

ACL Id (1-4096)	1	Block Id: 0 Group Id: 0
Filter Action	Deny	setCos value 0
Ethernet Packet Format	Disabled	
Tagging Packet Format	None	
Source MAC Address	00:00:00:00:00:00	Mask ff:ff:ff:ff:ff:ff
Destination MAC Address	00:00:00:00:00:00	Mask ff:ff:ff:ff:ff:ff
Ethernet Type	None	Value (0600-ffff) 0
VLAN Id (1-4095)	1	Mask (0-fff) fff
802.1p Priority	None	
Type of Service (0-255)	0	Disabled
Protocol (0-255)	0	Disabled
Source IP Address	0.0.0.0	Mask 255.255.255.255
Destination IP Address	100.10.1.116	Mask 255.255.255.255
TCP/UDP Src Port (1-65535)	1	Mask (0-ffff) ffff
TCP/UDP Dst Port (1-65535)	1	Mask (0-ffff) ffff
TCP Flags	<input type="checkbox"/> FIN <input type="checkbox"/> SYN <input type="checkbox"/> RST <input type="checkbox"/> PSH <input type="checkbox"/> ACK <input type="checkbox"/> URG Mask(0-3f) 3f	
Statistics	Disabled	
Egress port	None	

d. Click **Submit**.

2. Apply, verify, and save the configuration.



3. Add ACL 1 to port 1.
- Click the **Configure** context button on the Toolbar.
  - Select **Switch Ports** (click the underlined text, not the folder).

**Open** [p-Class GbE2 Switch](#)

**Select** [Switch Ports](#)

- [Port-Based Port Mirroring](#)
- [Layer 2](#)
- [RMON Menu](#)
- [Layer 3](#)
- [QoS](#)
- [Access Control](#)
- [Uplink Failure Detection](#)

- c. Select a port.

**Select** [1](#)

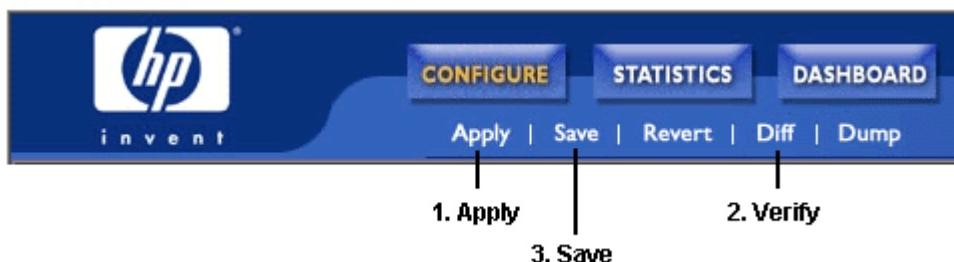
Switch Port	State	VLAN Tagging	Default PVID	PVID tagging	Multicast Threshold	Broadcast Threshold	Destination Lookup Fail Threshold	802.1p Priority
<a href="#">1</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0
<a href="#">2</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0
<a href="#">3</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0
<a href="#">4</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0
<a href="#">5</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0
<a href="#">6</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0
<a href="#">7</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0
<a href="#">8</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0
<a href="#">9</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0
<a href="#">10</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0

- d. Add the ACL to the port.

The screenshot shows the 'Switch Port 1 Configuration' screen. At the top, there is a 'Switch Port State' dropdown set to 'Enabled'. Below it is an 'ACL Configuration' section. This section contains four panels: 'ACLs Available' (containing ACL IDs 2 and 3), 'ACLs Selected' (containing ACL ID 1), 'ACL Blocks Available' (empty), 'ACL Blocks Selected' (empty), 'ACL Groups Available' (empty), and 'ACL Groups Selected' (empty). Between the 'Available' and 'Selected' panels for each category are 'Add >>' and '<< Remove' buttons. Vertical ellipses between sections indicate more configuration options below.

- e. Click **Submit**.

4. Apply, verify, and save the configuration.



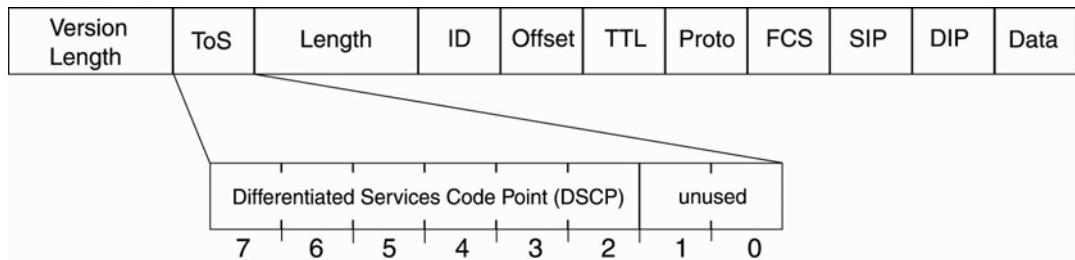
## Using DSCP values to provide QoS

The six most significant bits in the TOS byte of the IP header are defined as DiffServ Code Points (DSCP). Packets are marked with a certain value depending on the type of treatment the packet must receive in the network device. DSCP is a measure of the Quality of Service (QoS) level of the packet.

## Differentiated Services concepts

To differentiate between traffic flows, packets can be classified by their DSCP value. The Differentiated Services (DS) field in the IP header is an octet, and the first six bits, called the DS Code Point (DSCP), can provide QoS functions. Each packet carries its own QoS state in the DSCP. There are 64 possible DSCP values (0-63).

**Figure 12** Layer 3 IPv4 packet



## QoS levels

The following table shows the default service levels provided by the GbE2, listed from highest to lowest importance:

**Table 16** Default QoS service levels

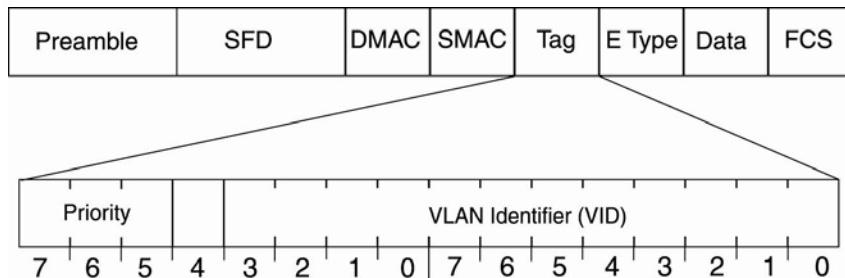
Service Level	Default PHB	802.1p Priority
Critical	CS7	7
Network Control	CS6	6
Premium	EF, CS5	5
Platinum	AF41, AF42, AF43, CS4	4
Gold	AF31, AF32, AF33, CS3	3
Silver	AF21, AF22, AF23, CS2	2
Bronze	AF11, AF12, AF13, CS1	1

## Using 802.1p priorities to provide QoS

GbE2 software provides Quality of Service functions based on the priority bits in a packet's VLAN header. (The priority bits are defined by the 802.1p standard within the IEEE 802.1q VLAN header.) The 802.1p bits, if present in the packet, specify the priority that should be given to packets during forwarding. Packets with a numerically higher (non-zero) priority are given forwarding preference over packets with lower priority.

The IEEE 802.1p standard uses eight levels of priority (0-7). Priority 7 is assigned to highest priority network traffic, such as OSPF or RIP routing table updates, priorities 5-6 are assigned to delay-sensitive applications such as voice and video, and lower priorities are assigned to standard applications. A value of 0 (zero) indicates a "best effort" traffic prioritization, and this is the default when traffic priority has not been configured on your network. The GbE2 can filter packets based on the 802.1p values, and it can assign or overwrite the 802.1p value in the packet.

**Figure 13** Layer 2 802.1q/802.1p VLAN tagged packet



Ingress packets receive a priority value, as follows:

- **Tagged packets**—GbE2 reads the 802.1p priority in the VLAN tag.
- **Untagged packets**—GbE2 tags the packet and assigns an 802.1p priority, based on the port's default priority (/cfg/port x/8021ppri).

Egress packets are placed in a COS queue based on the priority value, and scheduled for transmission based on the scheduling weight of the COS queue.

Use the /cfg/qos/8021p/cur command to display the mapping between 802.1p values, Class of Service queues (COSq), and COSq scheduling weights.

```
>> 802.1p# cur
Current priority to COS queue configuration:
Number of COSq: 8
Priority   COSq   Weight
-----  -----  -----
  0        0       1
  1        1       2
  2        2       3
  3        3       4
  4        4       5
  5        5       7
  6        6      15
  7        7       0
```

## 802.1p configuration (CLI example)

1. Configure a port's default 802.1 priority.

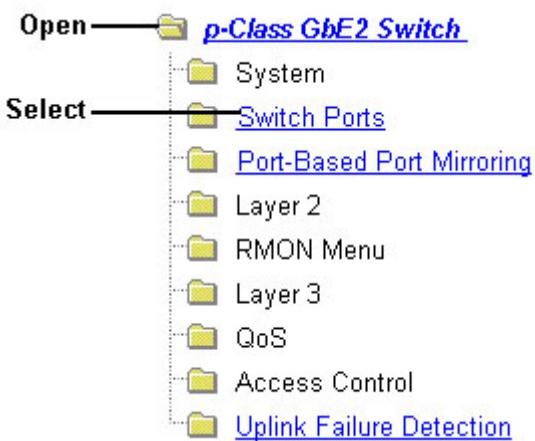
```
>> Main# cfg/port 19                                (Select port)
>> Port 19# 8021ppri                            (Set port's default 802.1p priority)
Current 802.1p priority: 0
Enter new 802.1p priority [0-7]: 1
>> Port 19# ena
>> Port 19# apply
```

2. Map the 802.1p priority value to a COS queue and set the COS queue scheduling weight.

```
>> Main# cfg/qos/8021p                           (Select 802.1p menu)
>> 802.1p# priq                                (Set COS queue assignments)
Enter priority [0-7]: 1
Current COS queue (for priority 1): 1
Enter new COS queue (for priority 1) [0-7]: 2
>> 802.1p# qweight                            (Set COS queue weights)
Enter COS queue [0-7]: 2
Current weight (for COS queue 2): 3
Enter new weight (for COS queue 2) [0-15]: 10
>> 802.1p# apply
```

## 802.1p configuration (BBI example)

1. Configure a port's default 802.1p priority.
  - a. Click the **Configure** context button on the Toolbar.
  - b. Select **Switch Ports** (click the underlined text, not the folder).



- c. Select a port.

Select [1](#)

Switch Ports Configuration									
Switch Port	State	VLAN Tagging	Default PVID	PVID tagging	Multicast Threshold	Broadcast Threshold	Destination Lookup Fail Threshold	802.1p Priority	
<a href="#">1</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0	
<a href="#">2</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0	
<a href="#">3</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0	
<a href="#">4</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0	
<a href="#">5</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0	
<a href="#">6</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0	
<a href="#">7</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0	
<a href="#">8</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0	
<a href="#">9</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0	
<a href="#">10</a>	enabled	disabled	1	enabled	disabled	disabled	disabled	0	

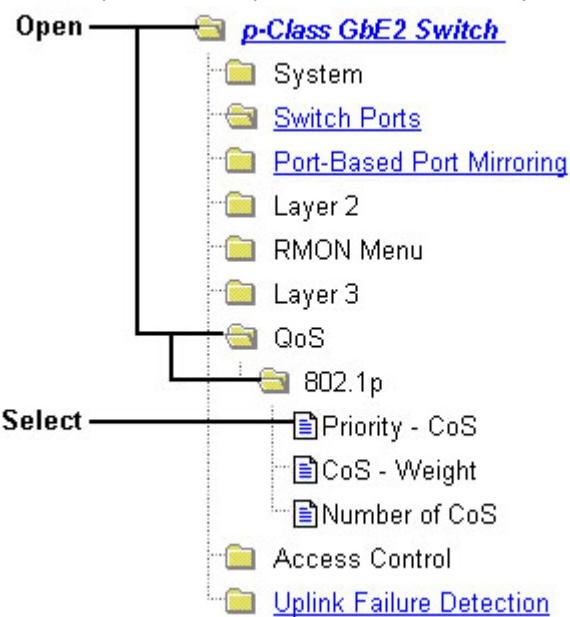
- d. Set the 802.1p priority value.

**Switch Port 1 Configuration**

Switch Port State	Enabled <input type="button" value="▼"/>
RMON Instrumentation	Disabled <input type="button" value="▼"/>
VLAN Tagging	Enabled <input type="button" value="▼"/>
PVID Tagging	Enabled <input type="button" value="▼"/>
Port STP	On <input type="button" value="▼"/>
Default Port VLAN ID (1 - 4095)	1
Flow Control	both Rx/Tx <input type="button" value="▼"/>
Autonegotiation	Enabled <input type="button" value="▼"/>
Speed	10/100/1000 <input type="button" value="▼"/>
Duplex Mode	Full/Half <input type="button" value="▼"/>
Enable/Disable sending Link UP/Down Trap	Enabled <input type="button" value="▼"/>
Port Name	Downlink1
Multicast Threshold	Disabled <input type="button" value="▼"/>
Multicast Threshold Rate (0-262143)	0
Broadcast Threshold	Disabled <input type="button" value="▼"/>
Broadcast Threshold Rate (0-262143)	0
Destination Lookup Fail Threshold	Disabled <input type="button" value="▼"/>
Destination Lookup Fail Threshold Rate (0-262143)	0
802.1p Port Priority (0-7)	2

- e. Click **Submit**.

2. Map the 802.1p priority value to a COS queue.
  - a. Click the **Configure** context button on the Toolbar.
  - b. Open the 802.1p folder, and select Priority - CoS.



- c. Select an 802.1p priority value.

**Priority CoS Configuration Table**

Priority	CoS
<u>0</u>	0
<u>1</u>	1
<u>2</u>	2
<u>3</u>	3
<u>4</u>	4
<u>5</u>	5
<u>6</u>	6
<u>7</u>	7

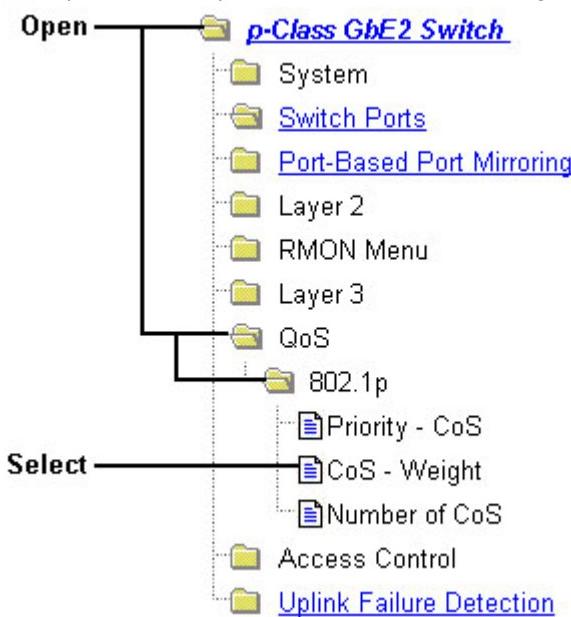
- d. Select a Class of Service queue (CoSQ) to correlate with the 802.1p priority value.

**CoSQ For Priority 1 Configuration**

CoSQ (0-7)	2
<b>Submit</b>	

- e. Click **Submit**.

3. Set the COS queue scheduling weight.
  - a. Click the **Configure** context button on the Toolbar.
  - b. Open the 802.1p folder, and select CoS - Weight.



- c. Select a Class of Service queue (CoS).

**CoS Weight Configuration Table**

CoS	Weight
0	1
1	2
2	3
3	4
4	5
5	7
6	15
7	0

- d. Enter a value for the weight of the Class of Service queue.

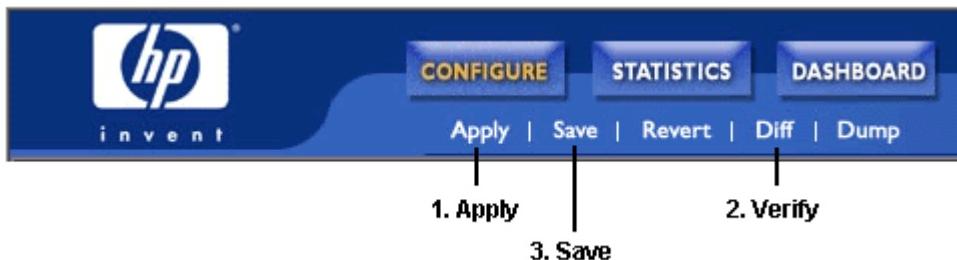
**CoSQ 2 Configuration**

CoSq Weight (0-15)	<input type="text" value="3"/>
--------------------	--------------------------------

**Submit**

- e. Click **Submit**.

- f. Apply, verify, and save the configuration.



## Queuing and scheduling

The GbE2 has eight output Class of Service queues (COSq) per port (0-7), into which each packet is placed. Each packet's 802.1p priority determines its COSq, except when an ACL action sets the COSq of the packet.

Class Of Service queues 0 - 6 use Weighted Round Robin (WRR) scheduling, with user configurable weight from 1 to 15. The weight of 0 (zero) indicates strict priority, which might starve the low priority queues. Queue 7 is a high-priority queue, and always has a weight of 0 (zero).

You can configure the following attributes for COS queues:

- Map 802.1p priority value to a COS queue.
- Define the scheduling weight of each COS queue.
- Define the number of COS queues available (2 or 8).

Use the 802.1p menu (/cfg/qos/8021p) to configure Class Of Service queues.

# Basic IP routing

This chapter provides configuration background and examples for using the GbE2 Interconnect Switch to perform IP routing functions. The following topics are addressed in this chapter:

- IP Routing Benefits
- Routing Between IP Subnets
- Example of Subnet Routing
- Defining IP Address Ranges for the Local Route Cache
- Dynamic Host Configuration Protocol

## IP routing benefits

The GbE2 Interconnect Switch uses a combination of configurable IP switch interfaces and IP routing options. The switch IP routing capabilities provide the following benefits:

- Connects the server IP subnets to the rest of the backbone network.
- Provides another means to invisibly introduce Jumbo frame technology into the server-switched network by automatically fragmenting UDP Jumbo frames when routing to non-Jumbo frame VLANs or subnets.
- Provides the ability to route IP traffic between multiple Virtual Local Area Networks (VLANs) configured on the switch.

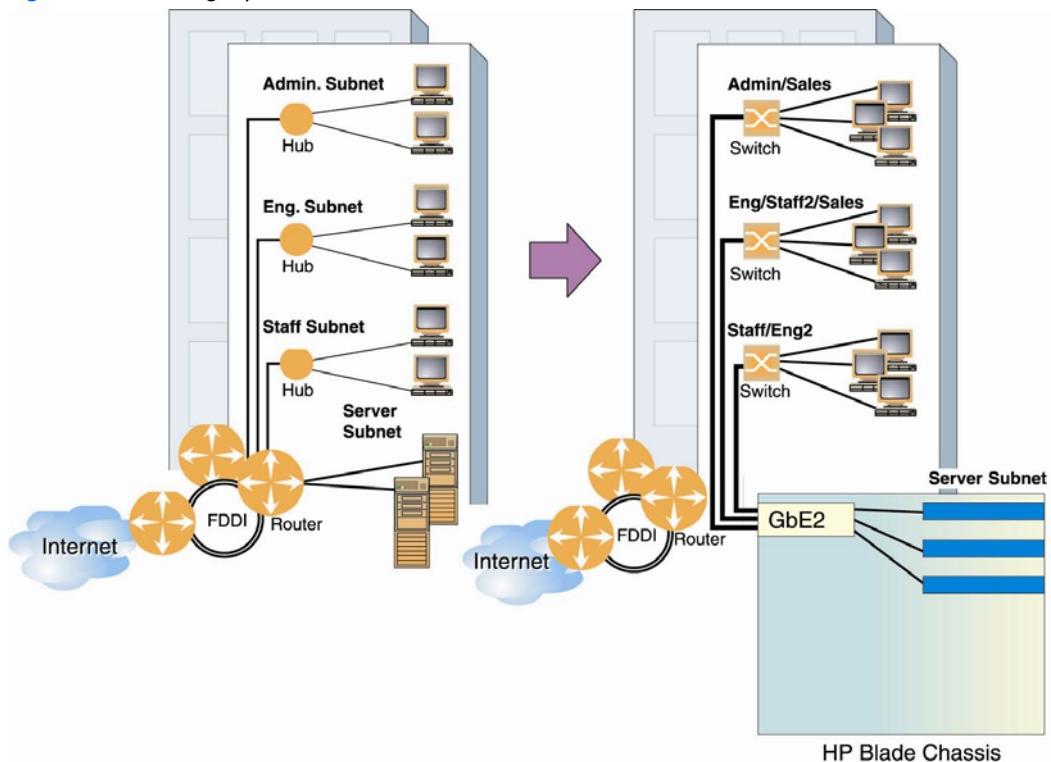
## Routing between IP subnets

The physical layout of most corporate networks has evolved over time. Classic hub/router topologies have given way to faster switched topologies, particularly now that switches are increasingly intelligent. GbE2 Interconnect Switches are intelligent and fast enough to perform routing functions on a par with wire speed Layer 2 switching.

The combination of faster routing and switching in a single device provides another service — it allows you to build versatile topologies that account for legacy configurations.

For example, consider the following topology migration:

**Figure 14** Router legacy network



In this example, a corporate campus has migrated from a router-centric topology to a faster, more powerful, switch-based topology. As is often the case, the legacy of network growth and redesign has left the system with a mix of illogically distributed subnets.

This is a situation that switching alone cannot cure. Instead, the router is flooded with cross-subnet communication. This compromises efficiency in two ways:

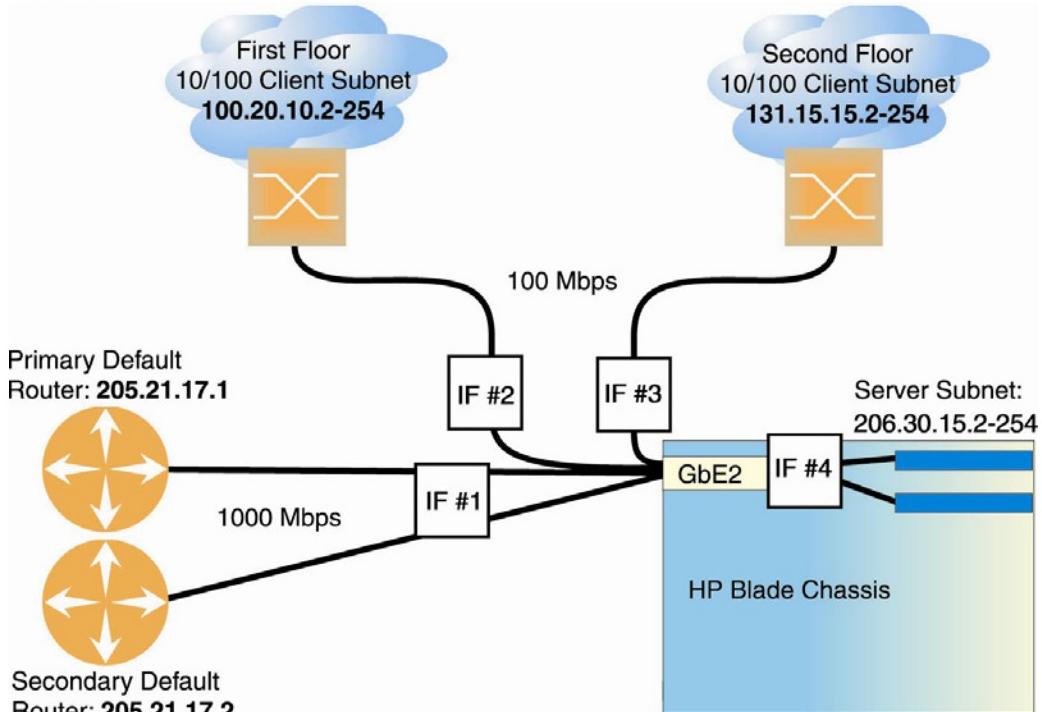
- Routers can be slower than switches. The cross-subnet side trip from the switch to the router and back again adds two hops for the data, slowing throughput considerably.
- Traffic to the router increases, increasing congestion.

Even if every end-station could be moved to better logical subnets (a daunting task), competition for access to common server pools on different subnets still burdens the routers.

This problem is solved by using GbE2 Interconnect Switches with built-in IP routing capabilities. Cross-subnet LAN traffic can now be routed within the switches with wire speed Layer 2 switching performance. This not only eases the load on the router but saves the network administrators from reconfiguring each and every end-station with new IP addresses.

Take a closer look at the GbE2 Interconnect Switch in the following configuration example:

**Figure 15** Switch-based routing topology



The GbE2 Interconnect Switch connects the Gigabit Ethernet and Fast Ethernet trunks from various switched subnets throughout one building. Common servers are placed on another subnet attached to the switch. Primary and backup routers are attached to the switch on yet another subnet.

Without Layer 3 IP routing on the switch, cross-subnet communication is relayed to the default gateway (in this case, the router) for the next level of routing intelligence. The router fills in the necessary address information and sends the data back to the switch, which then relays the packet to the proper destination subnet using Layer 2 switching.

With Layer 3 IP routing in place on the switch, routing between different IP subnets can be accomplished entirely within the switch. This leaves the routers free to handle inbound and outbound traffic for this group of subnets.

To make implementation even easier, UDP Jumbo frame traffic is automatically fragmented to regular Ethernet frame sizes when routing to non-Jumbo frame VLANs or subnets. This automatic frame conversion allows servers to communicate using Jumbo frames, all transparently to the user.

## Example of subnet routing

Prior to configuring, you must be connected to the switch Command Line Interface (CLI) as the administrator.



**NOTE:** For details about accessing and using any of the menu commands described in this example, see the *HP ProLiant BL p-Class GbE2 Interconnect Switch Command Reference Guide*.

1. Assign an IP address (or document the existing one) for each router and client workstation.

In the example topology, the following IP addresses are used:

**Table 17** Subnet routing example: IP address assignments

Subnet	Devices	IP Addresses
1	Primary and Secondary Default Routers	205.21.17.1 and 205.21.17.2
2	First Floor Client Workstations	100.20.10.2-254
3	Second Floor Client Workstations	131.15.15.2-254
4	Common Servers	206.30.15.2-254

2. Assign an IP interface for each subnet attached to the switch.

Since there are four IP subnets connected to the switch, four IP interfaces are needed

**Table 18** Subnet routing example: IP interface assignments

Interface	Devices	IP Interface Address
IF 1	Primary and Secondary Default Routers	205.21.17.3
IF 2	First Floor Client Workstations	100.20.10.1
IF 3	Second Floor Client Workstations	131.15.15.1
IF 4	Common Servers	206.30.15.1

IP interfaces are configured using the following commands at the CLI:

```
>> # /cfg/l3/if 1                                (Select IP interface 1)
>> IP Interface 1# addr 205.21.17.3              (Assign IP address)
>> IP Interface 1# ena                            (Enable IP interface 1)
>> IP Interface 1# ./if 2                          (Select IP interface 2)
>> IP Interface 2# addr 100.20.10.1              (Assign IP address)
>> IP Interface 2# ena                            (Enable IP interface 2)
>> IP Interface 2# ./if 3                          (Select IP interface 3)
>> IP Interface 3# addr 131.15.15.1              (Assign IP address)
>> IP Interface 3# ena                            (Enable IP interface 3)
>> IP Interface 3# ./if 4                          (Select IP interface 4)
>> IP Interface 4# addr 206.30.15.1              (Assign IP address)
>> IP Interface 4# ena                            (Enable IP interface 5)
```

3. Set each server and workstation's default gateway to the appropriate switch IP interface (the one in the same subnet as the server or workstation).

- Configure the default gateways to the routers' addresses.

Configuring the default gateways allows the switch to send outbound traffic to the routers:

>> IP Interface 5# .. /gw 1	(Select primary default gateway)
>> Default gateway 1# addr 205.21.17.1	(Assign IP address)
>> Default gateway 1# ena	(Enable primary default gateway)
>> Default gateway 1# .. /gw 2	(Select secondary default gateway)
>> Default gateway 2# addr 205.21.17.2	(Assign address)
>> Default gateway 2# ena	(Enable secondary default gateway)

- Enable, apply, and verify the configuration.

>> Default gateway 2# .. /fwrd	(Select the IP Forwarding Menu)
>> IP Forwarding# on	(Turn IP forwarding on)
>> IP Forwarding# apply	(Make your changes active)
>> IP Forwarding# /cfg/l3/cur	(View current IP settings)

Examine the resulting information. If any settings are incorrect, make the appropriate changes.

- Save your new configuration changes.

>> IP# save (Save for restore after reboot)
---

## Using VLANs to segregate broadcast domains

In the previous example, devices that share a common IP network are all in the same broadcast domain. If you want to limit the broadcasts on your network, you could use VLANs to create distinct broadcast domains. For example, as shown in the following procedure, you could create one VLAN for the client trunks, one for the routers, and one for the servers.

In this example, you are adding to the previous configuration.

- Determine which switch ports and IP interfaces belong to which VLANs.

The following table adds port and VLAN information:

**Table 19** Subnet routing example: Optional VLAN ports

VLAN	Devices	IP Interface	Switch Port	VLAN #
1	First Floor Client Workstations	2	19	1
	Second Floor Client Workstations	3	20	1
2	Primary Default Router	1	21	2
	Secondary Default Router	1	22	2
3	Common Servers 1	4	1	3
	Common Servers 2	4	2	3

**2.** Add the switch ports to their respective VLANs.

The VLANs shown in the table above are configured as follows:

```
>> # /cfg/l2/vlan 1(Select VLAN 1)
>> VLAN 1# add port 19          (Add port for 1st floor to VLAN 1)
>> VLAN 1# add port 20          (Add port for 2nd floor to VLAN 1)
>> VLAN 1# ena                 (Enable VLAN 1)
>> VLAN 1# ../VLAN 2           (Select VLAN 2)
>> VLAN 2# add port 21          (Add port for default router 1)
>> VLAN 2# add port 22          (Add port for default router 2)
>> VLAN 2# ena                 (Enable VLAN 2)
>> VLAN 2# ../VLAN 3           (Add port for default router 3)
>> VLAN 3# add port 1           (Select VLAN 3)
>> VLAN 3# add port 2           (Select port for common server 1)
>> VLAN 3# ena                 (Enable VLAN 3)
```

Each time you add a port to a VLAN, you may get the following prompt:

```
Port 4 is an untagged port and its current PVID is 1.
```

```
Confirm changing PVID from 1 to 2 [y/n] ?
```

Enter **y** to set the default Port VLAN ID (PVID) for the port.

**3.** Add each IP interface to the appropriate VLAN.

Now that the ports are separated into three VLANs, the IP interface for each subnet must be placed in the appropriate VLAN. The settings are made as follows:

```
>> VLAN 3# /cfg/l3/if 1         (Select IP interface 1 for def. routers)
>> IP Interface 1# vlan 2       (Set to VLAN 2)
>> IP Interface 1# ../if 2       (Select IP interface 2 for first floor)
>> IP Interface 2# vlan 1       (Set to VLAN 1)
>> IP Interface 2# ../if 3       (Select IP interface 3 for second floor)
>> IP Interface 3# vlan 1       (Set to VLAN 1)
>> IP Interface 3# ../if 4       (Select IP interface 4 for servers)
>> IP Interface 4# vlan 3       (Set to VLAN 3)
```

**4.** Apply and verify the configuration.

```
>> IP Interface 4# apply        (Make your changes active)
>> IP Interface 4# /info/vlan  (View current VLAN information)
>> Information# port           (View current port information)
```

Examine the resulting information. If any settings are incorrect, make the appropriate changes.

**5.** Save your new configuration changes.

```
>> Information# save          (Save for restore after reboot)
```

# Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is a transport protocol that provides a framework for automatically assigning IP addresses and configuration information to other IP hosts or clients in a large TCP/IP network. Without DHCP, the IP address must be entered manually for each network device. DHCP allows a network administrator to distribute IP addresses from a central point and automatically send a new IP address when a device is connected to a different place in the network.

DHCP is an extension of another network IP management protocol, Bootstrap Protocol (BOOTP), with an additional capability of being able to dynamically allocate reusable network addresses and configuration parameters for client operation.

Built on the client/server model, DHCP allows hosts or clients on an IP network to obtain their configurations from a DHCP server, thereby reducing network administration. The most significant configuration the client receives from the server is its required IP address; (other optional parameters include the "generic" file name to be booted, the address of the default gateway, and so forth).

The DHCP relay agent eliminates the need to have DHCP/BOOTP servers on every subnet. It allows the administrator to reduce the number of DHCP servers deployed on the network and to centralize them. Without the DHCP relay agent, there must be at least one DHCP server deployed at each subnet that has hosts needing to perform the DHCP request.

## DHCP relay agent

DHCP is described in RFC 2131, and the DHCP relay agent supported on GbE2 Interconnect Switches is described in RFC 1542. DHCP uses UDP as its transport protocol. The client sends messages to the server on port 67 and the server sends messages to the client on port 68.

DHCP defines the methods through which clients can be assigned an IP address for a finite lease period and allowing reassignment of the IP address to another client later. Additionally, DHCP provides the mechanism for a client to gather other IP configuration parameters it needs to operate in the TCP/IP network.

In the DHCP environment, the switch acts as a relay agent. The DHCP relay feature (/cfg/13/bootp) enables the switch to forward a client request for an IP address to two BOOTP servers with IP addresses that have been configured on the switch.

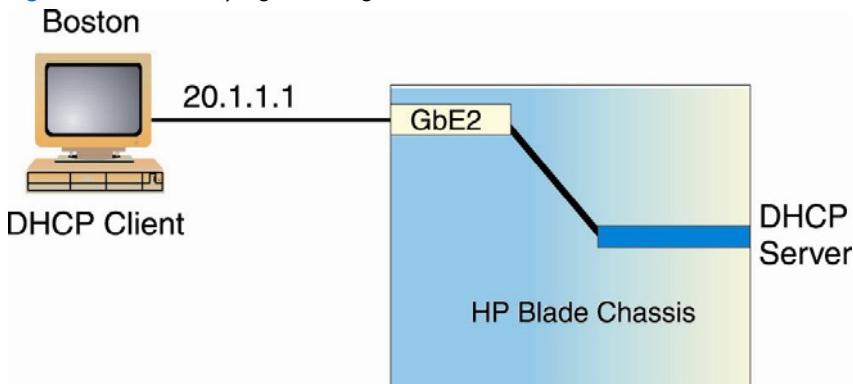
When a switch receives a UDP broadcast on port 67 from a DHCP client requesting an IP address, the switch acts as a proxy for the client, replacing the client source IP (SIP) and destination IP (DIP) addresses. The request is then forwarded as a UDP Unicast MAC layer message to two BOOTP servers whose IP addresses are configured on the switch. The servers respond as a UDP Unicast message back to the switch, with the default gateway and IP address for the client. The destination IP address in the server response represents the interface address on the switch that received the client request. This interface address tells the switch on which VLAN to send the server response to the client.

## DHCP relay agent configuration

To enable the switch to be the BOOTP forwarder, you need to configure the DHCP/BOOTP server IP addresses on the switch. Generally, you should configure the command on the switch IP interface closest to the client so that the DHCP server knows from which IP subnet the newly allocated IP address should come.

The following figure shows a basic DHCP network example:

**Figure 16** DHCP relay agent configuration



In GbE2 implementation, there is no need for primary or secondary servers. The client request is forwarded to the BOOTP servers configured on the switch. The use of two servers provides failover redundancy. However, no health checking is supported.

Use the following commands to configure the switch as a DHCP Relay Agent:

```
>> # /cfg/13/bootp
>> Bootstrap Protocol Relay# addr      (Set IP address of BOOTP server)
>> Bootstrap Protocol Relay# addr2     (Set IP address of 2nd BOOTP server)
>> Bootstrap Protocol Relay# on       (Globally turn BOOTP relay on)
>> Bootstrap Protocol Relay# off      (Globally turn BOOTP relay off)
>> Bootstrap Protocol Relay# cur      (Display current configuration)
```

DHCP Relay functionality can be assigned on a per interface basis. Use the following command to enable the Relay functionality:

```
>> # /cfg/13/if <interface number>/relay ena
```

# Routing Information Protocol

In a routed environment, routers communicate with one another to keep track of available routes. Routers can learn about available routes dynamically, using the Routing Information Protocol (RIP). GbE2 software supports RIP version 1 (RIPv1) and RIP version 2 (RIPv2) for exchanging TCP/IP route information with other routers.

## Distance vector protocol

RIP is known as a distance vector protocol. The vector is the network number and next hop, and the distance is the cost associated with the network number. RIP identifies network reachability based on cost, and cost is defined as hop count. One hop is considered to be the distance from one switch to the next which is typically 1. This cost or hop count is known as the metric.

When a switch receives a routing update that contains a new or changed destination network entry, the switch adds 1 to the metric value indicated in the update and enters the network in the routing table. The IP address of the sender is used as the next hop.

## Stability

RIP includes a number of other stability features that are common to many routing protocols. For example, RIP implements the split horizon and hold-down mechanisms to prevent incorrect routing information from being propagated.

RIP prevents routing loops from continuing indefinitely by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops in a path is 15. The network destination network is considered unreachable if increasing the metric value by 1 causes the metric to be 16 (that is infinity). This limits the maximum diameter of a RIP network to less than 16 hops.

RIP is often used in stub networks and in small autonomous systems that do not have many redundant paths.

## Routing updates

RIP sends routing-update messages at regular intervals and when the network topology changes. Each router "advertisers" routing information by sending a routing information update every 30 seconds. If a router doesn't receive an update from another router for 180 seconds, those routes provided by that router are declared invalid. After another 120 seconds without receiving an update for those routes, the routes are removed from the routing table and respective regular updates.

When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination.

For more information see The Configuration Menu, Routing Information Protocol Configuration ([/cfg/13/rip](#)) in the *HP ProLiant BL p-Class GbE2 Interconnect Switch Command Reference Guide*.

## RIPv1

RIP version 1 use broadcast User Datagram Protocol (UDP) data packets for the regular routing updates. The main disadvantage is that the routing updates do not carry subnet mask information. Hence, the router cannot determine whether the route is a subnet route or a host route. It is of limited usage after the introduction of RIPv2. For more information about RIPv1 and RIPv2, refer to RFC 1058 and RFC 2453.

## RIPv2

RIPv2 is the most popular and preferred configuration for most networks. RIPv2 expands the amount of useful information carried in RIP messages and provides a measure of security. For a detailed explanation of RIPv2, refer to RFC 1723 and RFC 2453.

RIPv2 improves efficiency by using multicast UDP (address 224.0.0.9) data packets for regular routing updates. Subnet mask information is provided in the routing updates. A security option is added for authenticating routing updates, by using a shared password. GbE2 software supports using clear password for RIPv2.

# RIPv2 in RIPv1 compatibility mode

GbE2 software allows you to configure RIPv2 in RIPv1 compatibility mode, for using both RIPv2 and RIPv1 routers within a network. In this mode, the regular routing updates use broadcast UDP data packet to allow RIPv1 routers to receive those packets. With RIPv1 routers as recipients, the routing updates have to carry natural or host mask. Hence, it is not a recommended configuration for most network topologies.



**NOTE:** When using both RIPv1 and RIPv2 within a network, use a single subnet mask throughout the network.

## RIP Features

GbE2 software provides the following features to support RIPv1 and RIPv2:

### Poison

Simple split horizon in RIP scheme omits routes learned from one neighbor in updates sent to that neighbor. That is the most common configuration used in RIP that is setting this Poison to disable. Split horizon with poisoned reverse includes such routes in updates, but sets their metrics to 16. The disadvantage of using this feature is the increase of size in the routing updates.

### Triggered updates

Triggered updates are an attempt to speed up convergence. When Triggered Updates is enabled (/cfg/l3/rip/if x/trigg ena), whenever a router changes the metric for a route, it sends update messages almost immediately, without waiting for the regular update interval. It is recommended to enable Triggered Updates.

### Multicast

RIPv2 messages use IP multicast address (224.0.0.9) for periodic broadcasts. Multicast RIPv2 announcements are not processed by RIPv1 routers. IGMP is not needed since these are inter-router messages which are not forwarded.

To configure RIPv2 in RIPv1-compatibility mode, set multicast to disable.

### Default

The RIP router can listen and supply a default route, usually represented as 0.0.0.0 in the routing table. When a router does not have an explicit route to a destination network in its routing table, it uses the default route to forward those packets.

### Metric

The metric field contains a configurable value between 1 and 15 (inclusive) which specifies the current metric for the interface. The metric value typically indicates the total number of hops to the destination. The metric value of 16 represents an unreachable destination.

### Authentication

RIPv2 authentication uses plaintext password for authentication. If configured using Authentication password, then it is necessary to enter an authentication key value.

The following method is used to authenticate a RIP message:

- If the router is not configured to authenticate RIPv2 messages, then RIPv1 and unauthenticated RIPv2 messages are accepted; authenticated RIPv2 messages are discarded.
- If the router is configured to authenticate RIPv2 messages, then RIPv1 messages and RIPv2 messages which pass authentication testing are accepted; unauthenticated and failed authentication RIPv2 messages are discarded.

For maximum security, RIPv1 messages are ignored when authentication is enabled (cfg/l3/rip/if x/auth password); otherwise, the routing information from authenticated messages is propagated by RIPv1 routers in an unauthenticated manner.

# RIP configuration example



**NOTE:** An interface RIP disabled uses all the default values of the RIP, no matter how the RIP parameters are configured for that interface. RIP sends out RIP regular updates to include an Up interface, but not a Down interface.

## 1. Add VLANs for routing interfaces.

```
>> Main# cfg/l2/vlan 2/ena          (Enable VLAN 2)
>> VLAN 2# add 20                  (Add port 20 to VLAN 2)

Port 20 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]: y

>> VLAN 2# /cfg/l2/vlan 3/ena      (Enable VLAN 3)
>> VLAN 3# add 21                  (Add port 21 to VLAN 3)

Port 21 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 3 [y/n]: y
```

## 2. Add IP interfaces to VLANs.

```
>> Main# cfg/l3/if 2/ena          (Enable interface 2)
>> IP Interface 2# addr 102.1.1.1  (Define IP address for interface 2)
>> IP Interface 2# vlan 2         (Add interface 2 to VLAN 2)
>> IP Interface 2# /cfg/l3/if 3/ena (Enable interface 3)
>> IP Interface 3# addr 103.1.1.1  (Define IP address for interface 3)
>> IP Interface 3# vlan 3         (Add interface 3 to VLAN 3)
```

## 3. Turn on RIP globally and enable RIP for each interface.

```
>> Main# cfg/l3/rip on           (Turn on RIP globally)
>> Routing Information Protocol# if 2/ena (Enable RIP on IP interface 2)
>> RIP Interface 2# ...
>> Routing Information Protocol# if 3/ena (Enable RIP on IP interface 3)
>> RIP Interface 3# apply        (Apply your changes)
>> RIP Interface 3# save        (Save the configuration)
```

Use the `/maint/route/dump` command to check the current valid routes in the routing table of the switch.

For those RIP learned routes, within the garbage collection period, that are routes phasing out of the routing table with metric 16, use the `/info/l3/rip/routes` command. Locally configured static routes do not appear in the RIP Routes table.

# IGMP Snooping

## Introduction

IGMP Snooping allows the switch to forward multicast traffic only to those ports that request it. IGMP Snooping prevents multicast traffic from being flooded to all ports. The switch learns which server hosts are interested in receiving multicast traffic, and forwards it only to ports connected to those servers.

The following topics are discussed in this chapter:

- Overview
- FastLeave
- IGMP Filtering
- Static Multicast Router
- IGMP Snooping Configuration example

## Overview

Internet Group Management Protocol (IGMP) is used by IP Multicast routers to learn about the existence of host group members on their directly attached subnet (see RFC 2236). The IP Multicast routers get this information by broadcasting IGMP Query Reports and listening for IP hosts reporting their host group memberships. This process is used to set up a client/server relationship between an IP Multicast source that provides the data streams and the clients that want to receive the data.

IGMP Snooping conserves bandwidth. With IGMP Snooping, the switch learns which ports are interested in receiving multicast data, and forwards multicast data only to those ports. In this way, other ports are not burdened with unwanted multicast traffic.

The switch currently supports snooping for IGMP version 1 and version 2.

The switch can sense IGMP Membership Reports from attached host servers and act as a proxy to set up a dedicated path between the requesting host and a local IP Multicast router. After the pathway is established, the switch blocks the IP Multicast stream from flowing through any port that does not connect to a host member, thus conserving bandwidth.

The client-server path is set up as follows:

- An IP Multicast Router (Mrouter) sends Membership Queries to the switch, which forwards them to all ports in a given VLAN.
- Hosts that want to receive the multicast data stream send Membership Reports to the switch, which sends a proxy Membership Report to the Mrouter.
- The switch sets up a path between the Mrouter and the host, and blocks all other ports from receiving the multicast.
- Periodically, the Mrouter sends Membership Queries to ensure that the host wants to continue receiving the multicast. If the host fails to respond with a Membership Report, the Mrouter stops sending the multicast to that path.
- The host can send a Leave report to the switch, which sends a proxy Leave report to the Mrouter. The multicast path is terminated immediately.

## FastLeave

When the switch with IGMP Snooping enabled receives an IGMPv2 leave message, it sends a Group-Specific Query to determine if any other devices in the same group (and on the same port) are still interested in the specified multicast group traffic. The switch removes the affiliated port from that particular group, if the following conditions apply:

- If the switch does not receive an IGMP Membership Report message within the query-response-interval
- If no multicast routers have been learnt on that port.

With Fastleave enabled on the VLAN, a port can be removed immediately from the port list of the group entry when the IGMP Leave message is received, unless a multicast router was learnt on the port.

Enable FastLeave only on VLANs that have only one host connected to each physical port.

## IGMP Filtering

With IGMP Filtering, you can allow or deny a port to send and receive multicast traffic to certain multicast groups. Unauthorized users are restricted from streaming multicast traffic across the network.

If access to a multicast group is denied, IGMP Membership Reports from the port for that group are dropped, and the port is not allowed to receive IP multicast traffic from that group. If access to the multicast group is allowed, Membership Reports from the port are forwarded for normal processing.

To configure IGMP Filtering, you must globally enable IGMP Filtering, define an IGMP Filter, assign the filter to a port, and enable IGMP Filtering on the port. To define an IGMP Filter, you must configure a range of IP multicast groups, choose whether the filter will allow or deny multicast traffic for groups within the range, and enable the filter.



**NOTE:** Low-numbered filters take precedence over high-number filters. For example, the action defined for IGMP Filter 1 supersedes the action defined for IGMP Filter 2.

### Configuring the range

Each IGMP Filter allows you to set a start and end point that defines the range of IP addresses upon which the filter takes action. Each IP address in the range must be between 224.0.0.0 and 239.255.255.255.

### Configuring the action

Each IGMP Filter can allow or deny IP multicasts to the range of IP addresses configured. If you configure the filter to deny IP multicasts, then IGMP Membership Reports from multicast groups within the range are dropped.

You can configure a secondary filter to allow IP multicasts to a small range of addresses within a larger range that a primary filter is configured to deny. The two filters work together to allow IP multicasts to a small subset of addresses within the larger range of addresses. The secondary filter must have a lower number than the primary filter, so that it takes precedence.

## Static multicast router

A static multicast router (Mrouter) can be configured for a particular port on a particular VLAN. A static Mrouter does not have to be learnt through IGMP Snooping.

A total of eight static Mrouters can be configured on the HP ProLiant BL p-Class GbE2 Interconnect Switch. Only uplink and interconnect ports (17-24) can accept a static Mrouter. A port that belongs to a trunk group cannot accept a static Mrouter, only Mrouters learnt through IGMP Snooping.

When you configure a static Mrouter on a VLAN, it replaces any dynamic Mrouters learnt through IGMP Snooping.

## IGMP Snooping configuration example

This section provides steps to configure IGMP Snooping on the HP ProLiant BL p-Class GbE2 Interconnect Switch, using the Command-Line Interface (CLI) or the Browser-Based Interface (BBI).

### Configuring IGMP Snooping (CLI example)

1. Configure port and VLAN membership on the switch, as described in the “Configuring Ports and VLANs (CLI example)” section in the “VLANs” chapter.
2. Add VLANs to IGMP Snooping and enable the feature.

>> /cfg/13/igmp/snoop	(Select IGMP Snoop menu)
>> IGMP Snoop# ena	(Enable IGMP Snooping)
>> IGMP Snoop# apply	(Make your changes active)

**3.** View dynamic IGMP information.

```
>> /info/l3/igmp                                (Select IGMP Information menu)
>> IGMP Multicast# dump                         (Show IGMP Group information)

>> Switch-A - IGMP Multicast# dump
      Group      VLAN     Version      Port
      -----  -----  -----
      238.1.0.0    1        V2          20
      238.1.0.1    1        V2          21

>> IGMP Multicast# mrouter                      (Select MRouter Information menu)
>> IGMP Multicast Router# dump                 (Show IGMP Group information)

      VLAN      Port      Version  L)earnt/(S)tatic
      -----  -----
      1            23        V2           S
```

These commands display information about IGMP Groups and Mrouters learned through IGMP Snooping.

## Configuring IGMP Filtering (CLI example)

**1.** Enable IGMP Filtering on the switch.

```
>> /cfg/l3/igmp/igmpflt                        (Select IGMP Filtering menu)
>> IGMP Filter# ena                            (Enable IGMP Filtering)
Current status: disabled
New status: enabled
```

**2.** Define an IGMP Filter.

```
>> //cfg/l3/igmp/igmpflt                      (Select IGMP Filtering menu)
>>IGMP Filter# filter 1                         (Select Filter 1 Definition menu)
>>IGMP Filter 1 Definition# range 224.0.1.0   (Enter first IP address of
the range)
Current multicast address2:
Enter new multicast address2: 226.0.0.0          (Enter second IP address)
Current multicast address1:
New pending multicast address1: 224.0.1.0
Current multicast address2:
New pending multicast address2: 226.0.0.0
>>IGMP Filter 1 Definition# action deny        (Deny multicast traffic)
>>IGMP Filter 1 Definition# ena                (Enable the filter)
```

**3.** Assign the IGMP Filter to a port.

```
>> //cfg/l3/igmp/igmpflt          (Select IGMP Filtering menu)
>>IGMP Filter# port 24           (Select port 24)
>>IGMP Port 24# filt ena        (Enable IGMP Filtering on the port)
Current port 24 filtering: disabled
New port 24 filtering: enabled
>>IGMP Port 24# add 1           (Add IGMP Filter 1 to the port)
>>IGMP Port 24# apply            (Make your changes active)
```

## Configuring a Static Mrouter (CLI example)

**1.** Configure a port to which the static Mrouter is connected, and enter the appropriate VLAN.

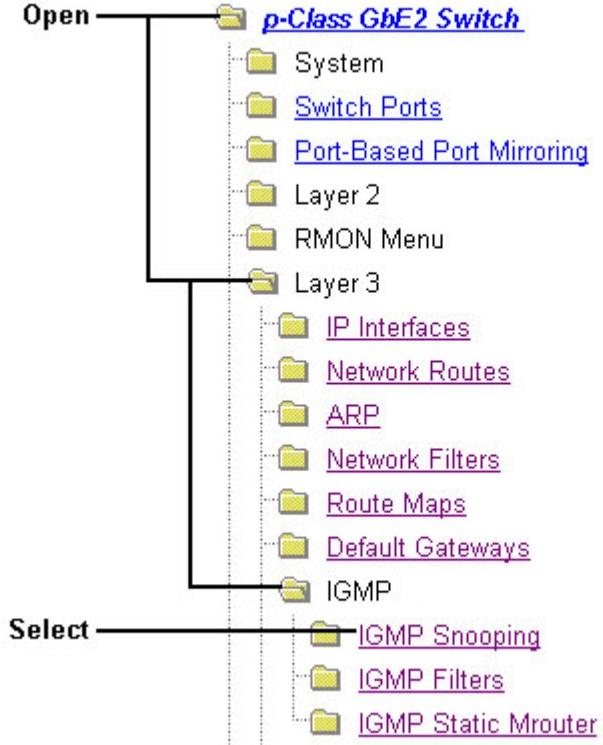
```
>> /cfg/l3/igmp/mrouter          (Select IGMP Mrouter menu)
>> Static Multicast Router# add 19 (Add port 19 as Static Mrouter port)
Enter VLAN number: (1-4095) 1      (Enter the VLAN number)
Enter the version number of mrouter [1|2]: 2 (Enter the IGMP
version number)
```

**2.** Apply, verify, and save the configuration.

```
>> Static Multicast Router# apply    (Apply the configuration)
>> Static Multicast Router# cur       (View the configuration)
>> Static Multicast Router# save     (Save the configuration)
```

## Configuring IGMP Snooping (BBI example)

1. Configure port and VLAN membership on the switch, as described in the “Configuring Ports and VLANs (BBI example)” section in the “VLANs” chapter.
2. Configure IGMP Snooping.
  - a. Click the **Configure** context button.
  - b. Open the IGMP folder, and select **IGMP Snooping** (click the underlined text, not the folder).



- c. Enable IGMP Snooping.

**IGMP Snooping Configuration**

IGMP on?	on <input type="button" value="▼"/>
Set report timeout	10
Set multicast router timeout	255
Set robust value or expected packet loss on subnet	2
Set query interval	125
Aggregate IGMP report	enabled <input type="button" value="▼"/>
Set Source IP for GSQ proxy	255.255.255.255
Remove all VLAN(s) from IGMP Snooping	none <input type="button" value="▼"/>

**Configured VLANs**

VLAN ID:#

VLAN:1  
VLAN:20  
VLAN:100

**Snooping VLANs**

VLAN ID:#

VLAN:134

**Snooping VLANs without Fstleave**

VLAN ID:#

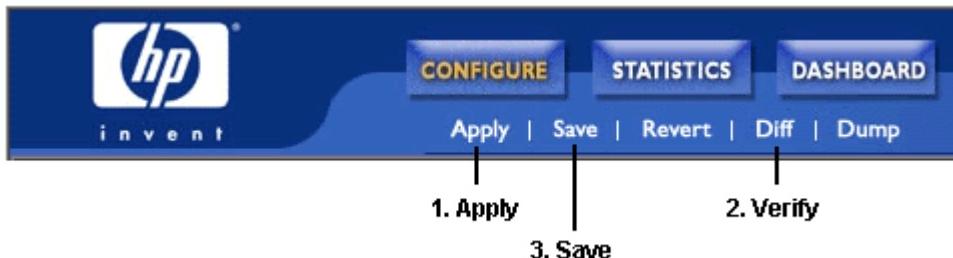
**Snooping VLANs with Fstleave**

VLAN ID:#

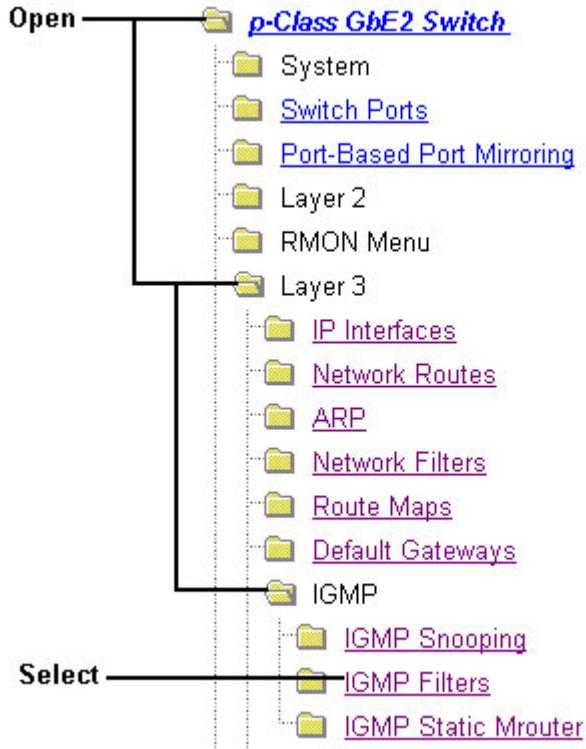
- d. Click **Submit**.

3. Apply, verify, and save the configuration.



## Configuring IGMP Filtering (BBI example)

1. Configure IGMP Snooping.
2. Enable IGMP Filtering.
  - a. Click the **Configure** context button.
  - b. Open the IGMP folder, and select **IGMP Filters** (click the underlined text, not the folder).



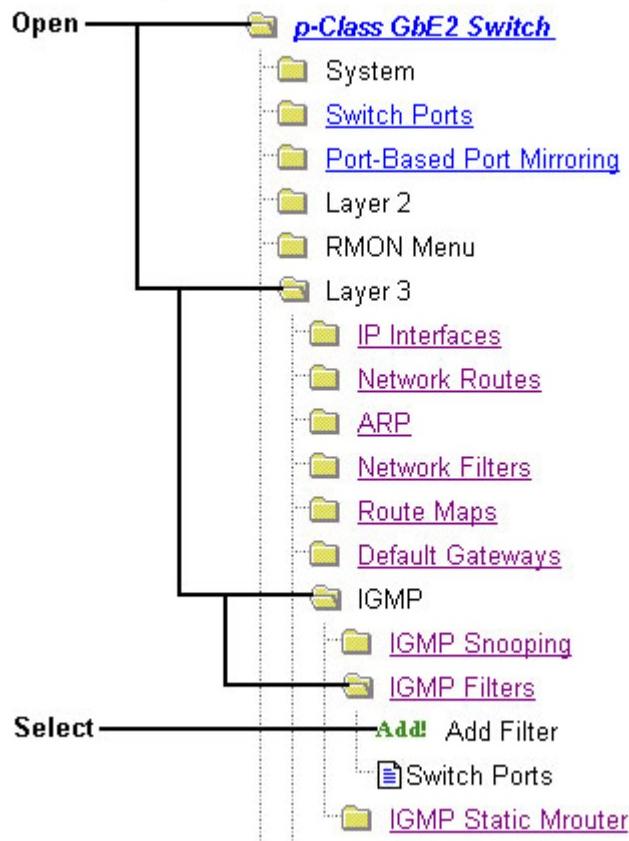
- c. Enable IGMP Filtering globally.

The dialog box title is 'IGMP Filters Configuration'. It contains a dropdown menu 'IGMP Filter Enabled?' set to 'Enabled' with a dropdown arrow. Below it is a 'Submit' button. A table below lists one filter entry:

Filter ID	Enabled?	Action	Range
1	ena	deny	224.0.1.0- 226.0.0.0

- d. Click **Submit**.

3. Define the IGMP Filter.
- a. Select Layer 3 > IGMP > IGMP Filters > **Add Filter**.



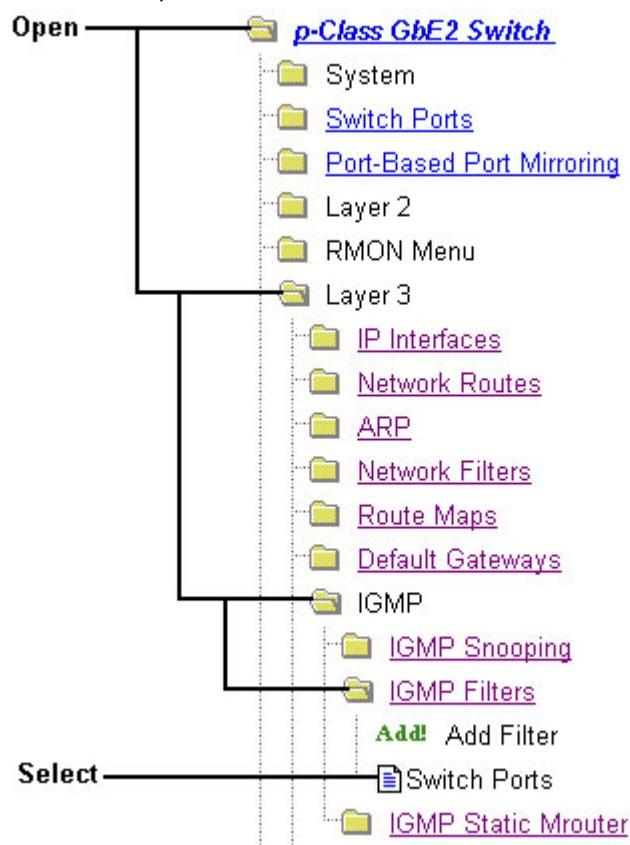
- b. Enable the IGMP Filter. Assign the range of IP multicast addresses and the filter action (allow or deny).

IGMP Filter Configuration	
Filter Identifier (1 - 16)	<input type="text" value="1"/>
Enabled?	<input checked="" type="checkbox"/>
Range 1 IP Multicast Address	<input type="text" value="224.0.1.0"/>
Range 2 IP Multicast Address	<input type="text" value="226.0.0.0"/>
Action	<input type="button" value="Deny"/>
<input type="button" value="Submit"/> <input type="button" value="Delete"/>	

- c. Click **Submit**.

4. Assign the filter to a port and enable IGMP Filtering on the port.

a. Select Layer 3 > IGMP > IGMP Filters > **Switch Ports**.



b. Select a port from the list.

IGMP Filtering Port Configuration	
Switch Port	IGMP Filter Processing?
<a href="#">1</a>	disabled
<a href="#">2</a>	disabled
<a href="#">3</a>	disabled
<a href="#">4</a>	disabled
⋮	
<a href="#">22</a>	disabled
<a href="#">23</a>	disabled
<a href="#">24</a>	disabled

**Select** → [24](#)

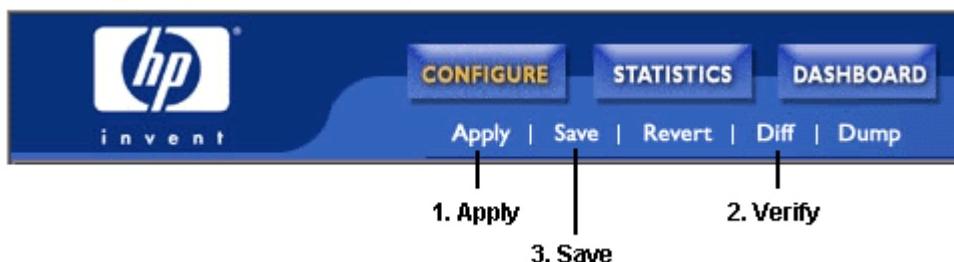
- c. Enable IGMP Filtering on the port. Select a filter in the IGMP Filters Available list, and click **Add**.

**IGMP Filtering - Port 24 Configuration**

Enable/Disable Filtering on Port <b>enabled</b>	
<b>IGMP Filters Available</b>	<b>IGMP Filters Selected</b>
<input type="text" value="Filter ID"/> <b>Add &gt;&gt;</b> <b>&lt;&lt; Remove</b>	<input type="text" value="Filter ID&lt;br/&gt;1"/>
<b>Submit</b>	

- d. Click **Submit**.

5. Apply, verify, and save the configuration.



### Configuring a Static Multicast Router (BBI example)

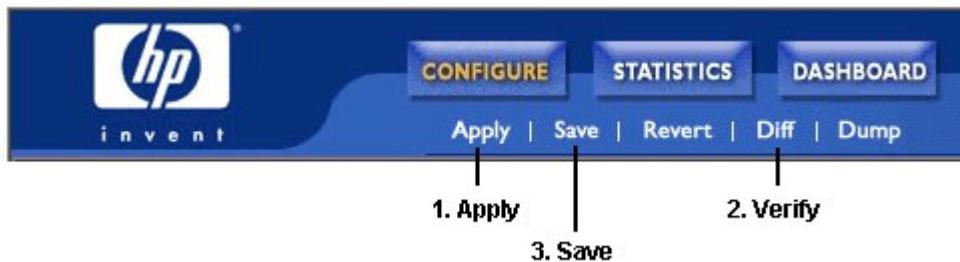
1. Configure Static Mrouter.
  - a. Click the **Configure** context button.
  - b. Open the Switch folder and select IP Menu > IGMP > **IGMP Static MRouter**.
  - c. Enter a port number, VLAN ID number, and IGMP version number.

**Static Multicast Router Configuration for Port**

<b>Mrouter Port ID (egs 1, 14..)</b>	<input type="text" value="20"/>
<b>Vlan ID</b>	<input type="text" value="1"/>
<b>IGMP Version?</b>	<b>Version2</b> <b>▼</b>
<b>Submit</b> <b>Delete</b>	

- d. Click **Submit**.

- 2.** Apply, verify, and save the configuration.



# OSPF

GbE2 software supports the Open Shortest Path First (OSPF) routing protocol. The GbE2 implementation conforms to the OSPF version 2 specifications detailed in Internet RFC 1583. The following sections discuss OSPF support for the GbE2 Interconnect Switch:

- OSPF Overview—This section provides information on OSPF concepts, such as types of OSPF areas, types of routing devices, neighbors, adjacencies, link state database, authentication, and internal versus external routing.
- OSPF Implementation in GbE2 Software—This section describes how OSPF is implemented in GbE2 software, such as configuration parameters, electing the designated router, summarizing routes, defining route maps and so forth.
- OSPF Configuration Examples—This section provides step-by-step instructions on configuring different configuration examples:
  - Creating a simple OSPF domain
  - Creating virtual links
  - Summarizing routes

## OSPF overview

OSPF is designed for routing traffic within a single IP domain called an Autonomous System (AS). The AS can be divided into smaller logical units known as *areas*.

All routing devices maintain link information in their own Link State Database (LSDB). The LSDB for all routing devices within an area is identical but is not exchanged between different areas. Only routing updates are exchanged between areas, thereby significantly reducing the overhead for maintaining routing information on a large, dynamic network.

The following sections describe key OSPF concepts.

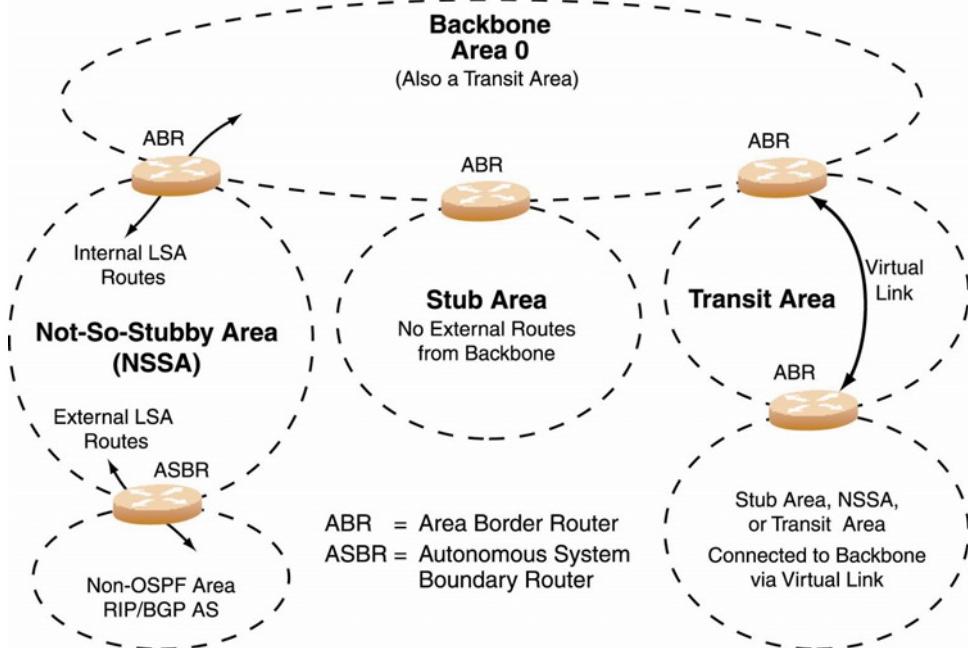
## Types of OSPF areas

An AS can be broken into logical units known as *areas*. In any AS with multiple areas, one area must be designated as area 0, known as the *backbone*. The backbone acts as the central OSPF area. All other areas in the AS must be connected to the backbone. Areas inject summary routing information into the backbone, which then distributes it to other areas as needed.

OSPF defines the following types of areas:

- Stub Area—an area that is connected to only one other area. External route information is not distributed into stub areas.
- Not-So-Stubby-Area (NSSA)—similar to a stub area with additional capabilities. Routes originating from within the NSSA can be propagated to adjacent transit and backbone areas. External routes from outside the AS can be advertised within the NSSA but are not distributed into other areas.
- Transit Area—an area that allows area summary information to be exchanged between routing devices. The backbone (area 0), any area that contains a virtual link to connect two areas, and any area that is not a stub area or an NSSA are considered transit areas

**Figure 17** OSPF area types

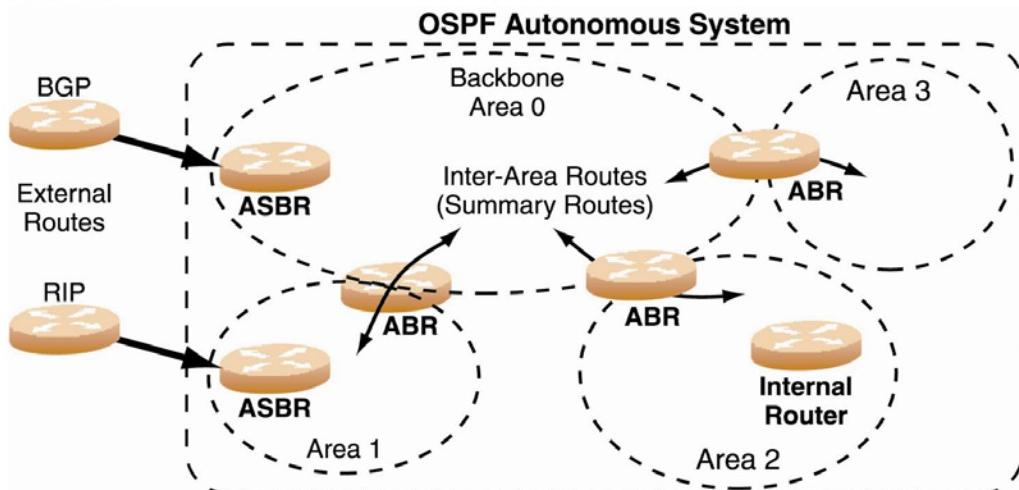


## Types of OSPF routing devices

As shown in the figure, OSPF uses the following types of routing devices:

- Internal Router (IR)—a router that has all of its interfaces within the same area. IRs maintain LSDBs identical to those of other routing devices within the local area.
- Area Border Router (ABR)—a router that has interfaces in multiple areas. ABRs maintain one LSDB for each connected area and disseminate routing information between areas.
- Autonomous System Boundary Router (ASBR)—a router that acts as a gateway between the OSPF domain and non-OSPF domains, such as RIP, BGP, and static routes.

**Figure 18** OSPF domain and an autonomous system



## Neighbors and adjacencies

In areas with two or more routing devices, *neighbors* and *adjacencies* are formed.

*Neighbors* are routing devices that maintain information about each others' health. To establish neighbor relationships, routing devices periodically send hello packets on each of their interfaces. All routing devices that share a common network segment, appear in the same area, and have the same health parameters (hello and dead intervals) and authentication parameters respond to each other's hello packets and become neighbors. Neighbors continue to send periodic hello packets to advertise their health to neighbors. In turn, they listen to hello packets to determine the health of their neighbors and to establish contact with new neighbors.

The hello process is used for electing one of the neighbors as the area's Designated Router (DR) and one as the area's Backup Designated Router (BDR). The DR is adjacent to all other neighbors and acts as the central contact for database exchanges. Each neighbor sends its database information to the DR, which relays the information to the other neighbors.

The BDR is adjacent to all other neighbors (including the DR). Each neighbor sends its database information to the BDR just as with the DR, but the BDR merely stores this data and does not distribute it. If the DR fails, the BDR will take over the task of distributing database information to the other neighbors.

## Link-State Database

OSPF is a link-state routing protocol. A *link* represents an interface (or routable path) from the routing device. By establishing an adjacency with the DR, each routing device in an OSPF area maintains an identical Link-State Database (LSDB) describing the network topology for its area.

Each routing device transmits a Link-State Advertisement (LSA) on each of its interfaces. LSAs are entered into the LSDB of each routing device. OSPF uses *flooding* to distribute LSAs between routing devices.

When LSAs result in changes to the routing device's LSDB, the routing device forwards the changes to the adjacent neighbors (the DR and BDR) for distribution to the other neighbors.

OSPF routing updates occur only when changes occur, instead of periodically. For each new route, if an adjacency is interested in that route (for example, if configured to receive static routes and the new route is indeed static), an update message containing the new route is sent to the adjacency. For each route removed from the route table, if the route has already been sent to an adjacency, an update message containing the route to withdraw is sent.

## Shortest Path First Tree

The routing devices use a link-state algorithm (Dijkstra's algorithm) to calculate the shortest path to all known destinations, based on the cumulative *cost* required to reach the destination.

The cost of an individual interface in OSPF is an indication of the overhead required to send packets across it. The cost is inversely proportional to the bandwidth of the interface. A lower cost indicates a higher bandwidth.

## Internal versus external routing

To ensure effective processing of network traffic, every routing device on your network needs to know how to send a packet (directly or indirectly) to any other location/destination in your network. This is referred to as *internal routing* and can be done with static routes or using active internal routing protocols, such as OSPF, RIP, or RIPv2.

It is also useful to tell routers outside your network (upstream providers or peers) about the routes you have access to in your network. Sharing of routing information between autonomous systems is known as *external routing*.

Typically, an AS will have one or more border routers (peer routers that exchange routes with other OSPF networks) as well as an internal routing system enabling every router in that AS to reach every other router and destination within that AS.

When a routing device *advertises* routes to boundary routers on other autonomous systems, it is effectively committing to carry data to the IP space represented in the route being advertised. For example, if the routing device advertises 192.204.4.0/24, it is declaring that if another router sends data destined for any address in the 192.204.4.0/24 range, it will carry that data to its destination.

# OSPF implementation in GbE2 software

The GbE2 Interconnect Switch supports a single instance of OSPF and up to 4 K routes on the network. The following sections describe OSPF implementation in GbE2 software:

- Configurable Parameters
- Defining Areas
- Interface Cost
- Electing the Designated Router and Backup
- Summarizing Routes
- Default Routes
- Virtual Links
- Router ID
- Authentication

## Configurable parameters

In GbE2 software, OSPF parameters can be configured through the Command Line Interface (CLI), Browser-Based Interface (BBI) for GbE2 Interconnect Switches, or through SNMP. For more information, see "Accessing the Switch."

The CLI supports the following parameters: interface output cost, interface priority, dead and hello intervals, retransmission interval, and interface transit delay.

OSPF traps—Traps produce messages upon certain events or error conditions, such as missing a hello, failing a neighbor, or recalculating the SPF.

In addition to the above parameters, you can also specify the following:

Link-State Database size—The size of the external LSA database can be specified to help manage the memory resources on the switch.

- Shortest Path First (SPF) interval—Time interval between successive calculations of the shortest path tree using the Dijkstra's algorithm.
- Stub area metric—A stub area can be configured to send a numeric metric value such that all routes received via that stub area carry the configured metric to potentially influence routing decisions.
- Default routes—Default routes with weight metrics can be manually injected into transit areas. This helps establish a preferred route when multiple routing devices exist between two areas. It also helps route traffic to external networks.

## Defining areas

If you are configuring multiple areas in your OSPF domain, one of the areas must be designated as area 0, known as the *backbone*. The backbone is the central OSPF area and is usually physically connected to all other areas. The areas inject routing information into the backbone which, in turn, disseminates the information into other areas.

Since the backbone connects the areas in your network, it must be a contiguous area. If the backbone is partitioned (possibly as a result of joining separate OSPF networks), parts of the AS will be unreachable, and you will need to configure *virtual links* to reconnect the partitioned areas (see "Virtual Links").

Up to three OSPF areas can be connected to the GbE2 Interconnect Switch. To configure an area, the OSPF number must be defined and then attached to a network interface on the switch. The full process is explained in the following sections.

An OSPF area is defined by assigning two pieces of information—an *area index* and an *area ID*. The command to define an OSPF area is as follows:

```
>> # /cfg/13/ospf/aindex <area index>/areaaid <n.n.n.n>
```

---

**NOTE:** The *aindex* option above is an arbitrary index used only on the switch and does not represent the actual OSPF area number. The actual OSPF area number is defined in the *areaaid* portion of the command as explained in the following sections.

---

## Assigning the area index

The `aindex <area index>` option is actually just an arbitrary index (0-2) used only by the switch. This index does not necessarily represent the OSPF area number, though for configuration simplicity, it should where possible.

For example, both of the following sets of commands define OSPF area 0 (the backbone) and area 1 because that information is held in the area ID portion of the command. However, the first set of commands is easier to maintain because the arbitrary area indexes agree with the area IDs:

- Area index and area ID agree
  - /cfg/l3/ospf/aindex 0/areaid 0.0.0.0(Use index 0 to set area 0 in ID octet format)
  - /cfg/l3/ospf/aindex 1/areaid 0.0.0.1(Use index 1 to set area 1 in ID octet format)
- Area index set to an arbitrary value
  - /cfg/l3/ospf/aindex 1/areaid 0.0.0.0(Use index 1 to set area 0 in ID octet format)
  - /cfg/l3/ospf/aindex 2/areaid 0.0.0.1(Use index 2 to set area 1 in ID octet format)

## Using the area ID to assign the OSPF area number

The OSPF area number is defined in the `areaid <IP address>` option. The octet format is used in order to be compatible with two different systems of notation used by other OSPF network vendors. There are two valid ways to designate an area ID:

- Placing the area number in the last octet (0.0.0.*n*)  
Most common OSPF vendors express the area ID number as a single number. For example, the Cisco IOS-based router command “network 1.1.1.0 0.0.0.255 area 1” defines the area number simply as “area 1”. On the GbE2, using the last octet in the area ID, “area 1” is equivalent to “areaid 0.0.0.1”.
- Multi-octet (<IP address>)  
Some OSPF vendors express the area ID number in multi-octet format. For example, “area 2.2.2.2” represents OSPF area 2 and can be specified directly on the GbE2 as “areaid 2.2.2.2”.

**NOTE:** Although both types of area ID formats are supported, be sure that the area IDs are in the same format throughout an area.

## Attaching an area to a network

Once an OSPF area has been defined, it must be associated with a network. To attach the area to a network, you must assign the OSPF area index to an IP interface that participates in the area. The format for the command is as follows:

```
>> # /cfg/l3/ospf/if <interface number>/aindex <area index>
```

For example, the following commands could be used to configure IP interface 14 for a presence on the 10.10.10.1/24 network, to define OSPF area 1, and to attach the area to the network:

```
>> # /cfg/13/if 14          (Select menu for IP interface 14)
      IP Interface 14# addr 10.10.10.1 (Define IP address on
      backbone
      network)
      IP Interface 14# mask 255.255.255.0 (Define IP mask on
      backbone)
      IP Interface 14# ena           (Enable IP interface 14)
      IP Interface 14# ../ospf/aindex 1 (Select menu for area index
      1)
      OSPF Area (index) 1 # areaid 0.0.0.1 (Define area ID as OSPF
      area 1)
      OSPF Area (index) 1 # ena       (Enable area index 1)
      OSPF Area (index) 1 # ../if 14  (Select OSPF menu for
      interface 14)
      OSPF Interface 14# aindex 1    (Attach area to network on
      interface 14)
      OSPF Interface 14# enable     (Enable interface 14 for area
      index 1)
```

## Interface cost

The OSPF link-state algorithm (Dijkstra's algorithm) places each routing device at the root of a tree and determines the cumulative *cost* required to reach each destination. Usually, the cost is inversely proportional to the bandwidth of the interface. Low cost indicates high bandwidth. You can manually enter the cost for the output route with the following command:

```
>> # /cfg/13/ospf/if <OSPF interface number>/cost <cost value
(1-65535) >
```

## Electing the designated router and backup

In any area with more than two routing devices, a Designated Router (DR) is elected as the central contact for database exchanges among neighbors, and a Backup Designated Router (BDR) is elected in case the DR fails.

DR and BDR elections are made through the hello process. The election can be influenced by assigning a priority value to the OSPF interfaces on the switch. The command is as follows:

```
>>#/cfg/13/ospf/if <OSPF interface number>/prio <priorty value
(0-255) >
```

A priority value of 255 is the highest, and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as a DR or BDR. In case of a tie, the routing device with the lowest router ID wins.

## Summarizing routes

Route summarization condenses routing information. Without summarization, each routing device in an OSPF network would retain a route to every subnet in the network. With summarization, routing devices can reduce some sets of routes to a single advertisement, reducing both the load on the routing device and the perceived complexity of the network. The importance of route summarization increases with network size.

Summary routes can be defined for up to 16 IP address ranges using the following command:

```
>> # /cfg/13/ospf/range <range number>/addr <IP address>/mask
<mask>
```

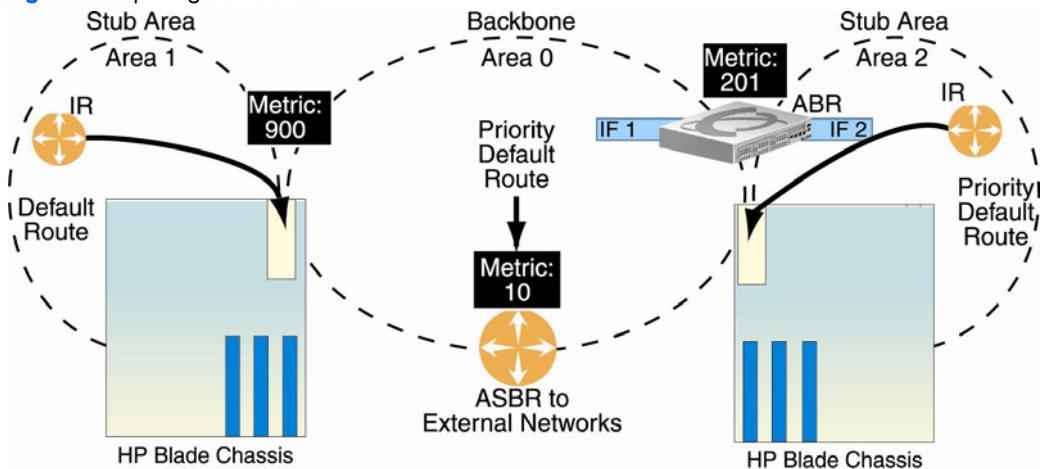
where <range number> is a number 1 to 16, <IP address> is the base IP address for the range, and <mask> is the IP address mask for the range.

## Default routes

When an OSPF routing device encounters traffic for a destination address it does not recognize, it forwards that traffic along the *default route*. Typically, the default route leads upstream toward the backbone until it reaches the intended area or an external router.

Each switch acting as an ABR automatically inserts a default route into each attached area. In simple OSPF stub areas or NSSAs with only one ABR leading upstream (see Area 1 in the figure below), any traffic for IP address destinations outside the area is forwarded to the switch's IP interface, and then into the connected transit area (usually the backbone). Since this is automatic, no further configuration is required for such areas.

**Figure 19** Injecting default routes



In more complex OSPF areas with multiple ABRs or ASBRs (such as area 0 and area 2 in the figure), there are multiple routes leading from the area. In such areas, traffic for unrecognized destinations cannot tell which route leads upstream without further configuration.

To resolve the situation and select one default route among multiple choices in an area, you can manually configure a metric value on each ABR. The metric assigns a priority to the ABR for its selection as the priority default route in an area. The following command is used for setting the metric value:

```
>> # /cfg/l3/ospf/default <metric value> <metric type (1 or 2)>
```

where *<metric value>* sets the priority for choosing this switch for default route. The value *none* sets no default and 1 sets the highest priority for default route. Metric type determines the method for influencing routing decisions for external routes.

To clear a default route metric from the switch, use the following command:

```
>> # /cfg/l3/ospf/default none
```

## Virtual links

Usually, all areas in an OSPF AS are physically connected to the backbone. In some cases where this is not possible, you can use a *virtual link*. Virtual links are created to connect one area to the backbone through another non-backbone area.

The area which contains a virtual link must be a transit area and have full routing information. Virtual links cannot be configured inside a stub area or NSSA. The area type must be defined as *transit* using the following command:

```
>> # /cfg/l3/ospf/aindex <area index>/type transit
```

The virtual link must be configured on the routing devices at each endpoint of the virtual link, though they may traverse multiple routing devices. To configure a switch as one endpoint of a virtual link, use the following command:

```
>> # /cfg/l3/ospf/virt <link number>/aindex <area index>/nbr <router ID>
```

where *<link number>* is a value between 1 and 3, *<area index>* is the OSPF area index of the transit area, and *<router ID>* is the IP address of the virtual neighbor (nbr), the routing device at the target endpoint. Another router ID is needed when configuring a virtual link in the other direction. To provide the switch with a router ID, see "Router ID."

For a detailed configuration example on Virtual Links, see "Example 2: Virtual Links."

## Router ID

Routing devices in OSPF areas are identified by a router ID. The router ID is expressed in IP address format. The IP address of the router ID is not required to be included in any IP interface range or in any OSPF area.

The router ID can be configured in one of the following two ways:

- Dynamically—OSPF protocol configures the lowest IP interface IP address as the router ID. This is the default.
- Statically—Use the following command to manually configure the router ID

```
>> # /cfg/l3/rtrid <IP address>
```

To modify the router ID from static to dynamic, set the router ID to 0.0.0.0, save the configuration, and reboot the switch. To view the router ID, enter:

```
>> # /info/l3/ospf/gen
```

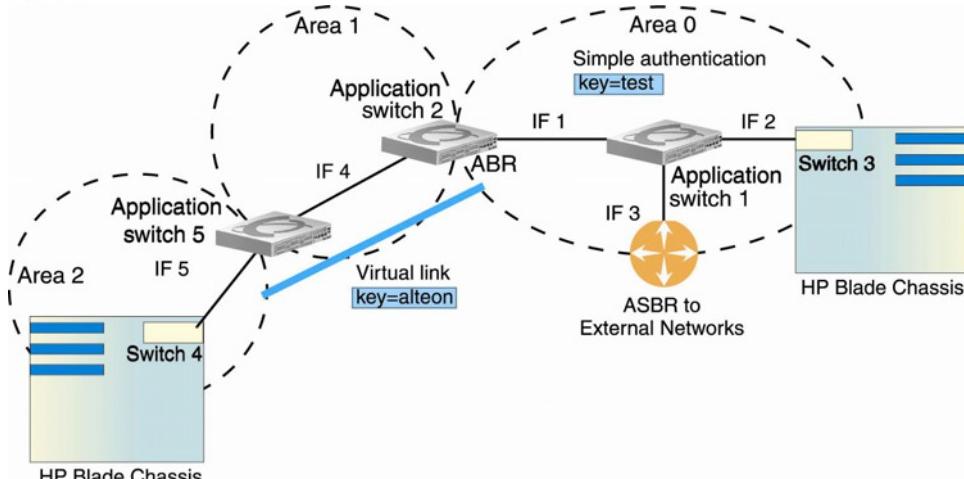
## Authentication

OSPF protocol exchanges can be authenticated so that only trusted routing devices can participate. This ensures less processing on routing devices that are not listening to OSPF packets.

OSPF allows packet authentication and uses IP multicast when sending and receiving packets. Routers participate in routing domains based on predefined passwords. GbE2 software supports simple password (type 1 plain text passwords) and MD5 cryptographic authentication. This type of authentication allows a password to be configured per area.

The following figure shows authentication configured for area 0 with the password test. Simple authentication is also configured for the virtual link between area 2 and area 0. Area 1 is not configured for OSPF authentication.

**Figure 20** OSPF authentication



To configure simple plain text OSPF passwords on the switches shown in the figure use the following commands:

1. Enable OSPF authentication for Area 0 on switches 1, 2, and 3.

```
>> # /cfg/l3/ospf/aindex 0/auth password
```

2. Configure a simple text password up to eight characters for each OSPF IP interface in Area 0 on switches 1, 2, and 3.

```
>> # /cfg/l3/ospf/if 1
>> OSPF Interface 1 # key test
>> OSPF Interface 1 # ../if 2
>> OSPF Interface 2 # key test
>> OSPF Interface 1 # ../if 3
>> OSPF Interface 3 # key test
```

3. Enable OSPF authentication for Area 2 on switch 4.

```
>> # /cfg/l3/ospf/aindex 2/auth password
```

4. Configure a simple text password up to eight characters for the virtual link between Area 2 and Area 0 on switches 2 and 4.

```
>> # /cfg/l3/ospf/virt 1/key packard
```

Use the following commands to configure MD5 authentication on the switches shown in the figure:

1. Enable OSPF MD5 authentication for Area 0 on switches 1, 2, and 3

```
>> # /cfg/l3/ospf/aindex 0/auth md5
```

2. Configure MD5 key ID for Area 0 on switches 1, 2, and 3.

```
>> # /cfg/l3/ospf/md5key 1/key test
```

3. Assign MD5 key ID to OSPF interfaces on switches 1, 2, and 3.

```
>> # /cfg/l3/ospf/if 1
>> OSPF Interface 1 # mdkey 1
>> OSPF Interface 1 # ../if 2
>> OSPF Interface 2 # mdkey 1
>> OSPF Interface 1 # ../if 3
>> OSPF Interface 3 # mdkey 1
```

4. Enable OSPF MD5 authentication for Area 2 on switch 4.

```
>> # /cfg/l3/ospf/aindex 2/auth md5
```

5. Configure MD5 key for the virtual link between Area 2 and Area 0 on switches 2 and 4.

```
>> # /cfg/l3/ospf/md5key 2/key packard
```

6. Assign MD5 key ID to OSPF virtual link on switches 2 and 4.

```
>> # /cfg/l3/ospf/virt 1/mdkey 2
```

## Host routes for load balancing

GbE2 software implementation of OSPF includes host routes. Host routes are used for advertising network device IP addresses to external networks, accomplishing the following goals:

- ABR Load Sharing**

As a form of load balancing, host routes can be used for dividing OSPF traffic among multiple ABRs. To accomplish this, each switch provides identical services but advertises a host route for a different IP address to the external network. If each IP address serves a different and equal portion of the external world, incoming traffic from the upstream router should be split evenly among ABRs.

- ABR Failover**

Complementing ABR load sharing, identical host routes can be configured on each ABR. These host routes can be given different costs so that a different ABR is selected as the preferred route for each server and the others are available as backups for failover purposes.

- **Equal Cost Multipath (ECMP)**

With equal cost multipath, a router potentially has several available next hops towards any given destination. ECMP allows separate routes to be calculated for each IP Type of Service. All paths of equal cost to a given destination are calculated, and the next hops for all equal-cost paths are inserted into the routing table.

If redundant routes via multiple routing processes (such as OSPF, RIP, BGP, or static routes) exist on your network, the switch defaults to the OSPF-derived route.

## OSPF features not supported in this release

The following OSPF features are not supported in this release:

- Summarizing external routes
- Filtering OSPF routes
- Using OSPF to forward multicast routes
- Configuring OSPF on non-broadcast multi-access networks (such as frame relay, X.25, and ATM)

## OSPF configuration examples

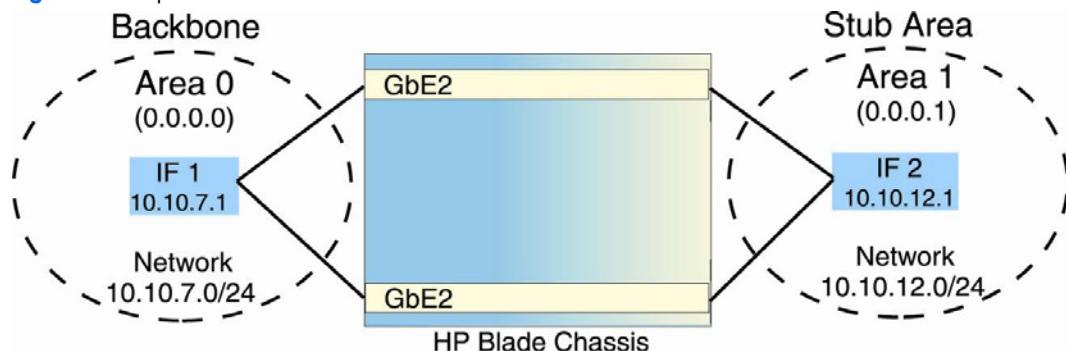
A summary of the basic steps for configuring OSPF on the GbE2 Interconnect Switch is listed here. Detailed instructions for each of the steps is covered in the following sections:

- Configure IP interfaces.  
One IP interface is required for each desired network (range of IP addresses) being assigned to an OSPF area on the switch.
- (Optional) Configure the router ID.  
The router ID is required only when configuring virtual links on the switch.
- Enable OSPF on the switch.
- Define the OSPF areas.
- Configure OSPF interface parameters.  
IP interfaces are used for attaching networks to the various areas.
- (Optional) Configure route summarization between OSPF areas.
- (Optional) Configure virtual links.
- (Optional) Configure host routes.

## Example 1: Simple OSPF domain (CLI example)

In this example, two OSPF areas are defined—one area is the backbone and the other is a stub area. A stub area does not allow advertisements of external routes, thus reducing the size of the database. Instead, a default summary route of IP address 0.0.0.0 is automatically inserted into the stub area. Any traffic for IP address destinations outside the stub area will be forwarded to the stub area's IP interface, and then into the backbone.

**Figure 21** Simple OSPF domain



Follow this procedure to configure OSPF support as shown in the figure.

**1. Configure IP interfaces on each network that will be attached to OSPF areas.**

In this example, two IP interfaces are needed: one for the backbone network on 10.10.7.0/24 and one for the stub area network on 10.10.12.0/24.

```
>> # /cfg/13/if 1 (Select menu for IP interface 1)
>> IP Interface 1 # addr 10.10.7.1(Set IP address on backbone network)
>> IP Interface 1 # mask 255.255.255.0(Set IP mask on backbone network)
>> IP Interface 1 # enable(Enable IP interface 1)
>> IP Interface 1 # ../if 2>Select menu for IP interface 2)
>> IP Interface 2 # addr 10.10.12.1(Set IP address on stub area network)
>> IP Interface 2 # mask 255.255.255.0(Set IP mask on stub area network)
>> IP Interface 2 # enable(Enable IP interface 2)
```

**2. Enable OSPF.**

```
>> IP Interface 2 # /cfg/13/ospf/on(Enable OSPF on the switch)
```

**3. Define the backbone.**

The backbone is always configured as a transit area using areaid 0.0.0.0

```
>> Open Shortest Path First # aindex 0>Select menu for area index 0)
>> OSPF Area (index) 0 # areaid 0.0.0.0(Set the ID for backbone area 0)
>> OSPF Area (index) 0 # type transit(Define backbone as transit type)
>> OSPF Area (index) 0 # enable(Enable the area)
```

**4. Define the stub area.**

```
>> OSPF Area (index) 0 # ../aindex 1>Select menu for area index 1)
>> OSPF Area (index) 1 # areaid 0.0.0.1(Set the area ID for OSPF area 1)
>> OSPF Area (index) 1 # type stub(Define area as stub type)
>> OSPF Area (index) 1 # enable(Enable the area)
```

**5. Attach the network interface to the backbone.**

```
>> OSPF Area 1 # ../if 1 (Select OSPF menu for IP interface 1)
>> OSPF Interface 1 # aindex 0(Attach network to backbone index)
>> OSPF Interface 1 # enable(Enable the backbone interface)
```

**6. Attach the network interface to the stub area.**

```
>> OSPF Interface 1 # ../if 2>Select OSPF menu for IP interface 2)
>> OSPF Interface 2 # aindex 1(Attach network to stub area index)
>> OSPF Interface 2 # enable(Enable the stub area interface)
```

**7. Apply and save the configuration changes.**

```
>> OSPF Interface 2 # apply(Global command to apply all changes)
>> OSPF Interface 2 # save(Global command to save all changes)
```

## Example 1: Simple OSPF domain (BBI example)

1. Configure IP interfaces on each network that will be attached to OSPF areas:

- IF 1  
IP address = 10.10.7.1  
Subnet mask = 255.255.255.0
- IF 2  
IP address = 10.10.12.1  
Subnet mask = 255.255.255.0

- a. Click the **Configure** context button.
- b. Open the IP Interfaces folder, and select **Add IP Interface**.

**Open** —   
p-Class GbE2 Switch  
System  
Switch Ports  
Port-Based Port Mirroring  
Layer 2  
RMON Menu  
Layer 3  
IP Interfaces

**Select** —   
**Add IP Interface**

**c.** Configure an IP interface. Enter the IP address, subnet mask, and enable the interface.

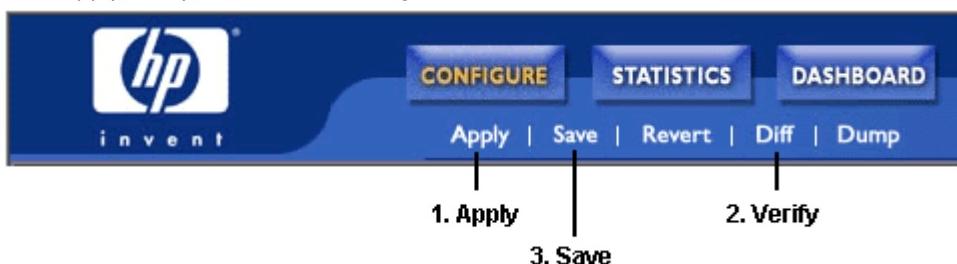
**IP Interface Configuration**

IP Interface Identifier (1-255)	1
IP Address	10.10.7.1
Enabled?	Enabled
Subnet Mask	255.255.255.0
Broadcast Address	
VLAN Membership ID (1 - 4095)	1
Enable/Disable BOOTP Relay	Enabled

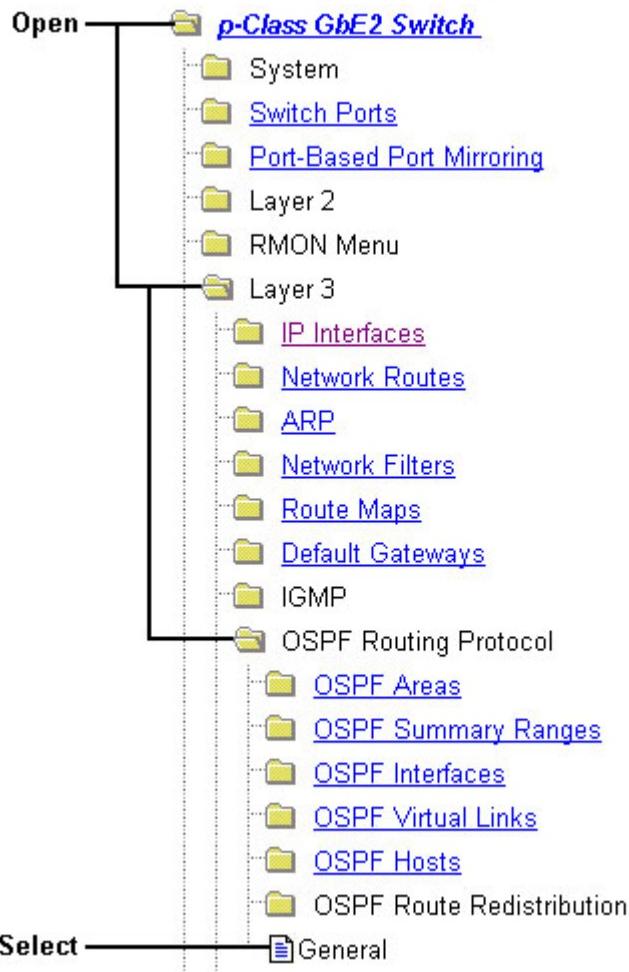
Submit    Delete

- d. Click **Submit**.

2. Apply, verify, and save the configuration.



3. Enable OSPF.
- Open the OSPF Routing Protocol folder, and select **General**.



- Enable OSPF.

**OSPF General Configuration**

Globally Enable OSPF ?	<input checked="" type="button"/> enabled
External LSDB Limit (0-2000)	<input type="text"/> 0
Default Route Metric (1-16777215, 0=none)	<input type="text"/> 0
Default Route Metric Type	<input type="button"/> none

**OSPF MD5 Keys Configuration**

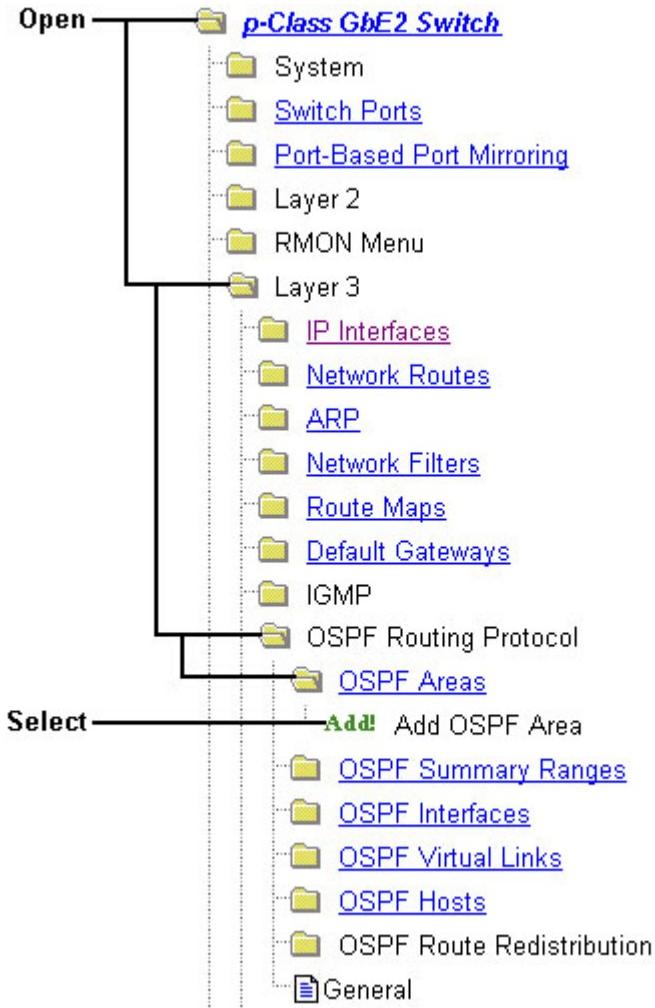
ID	MD5 Key

**Submit**

**Add OSPF Mdkey**

- Click **Submit**.

4. Configure OSPF Areas.
- Open the OSPF Areas folder, and select **Add OSPF Area**.



- Configure the OSPF backbone area 0.

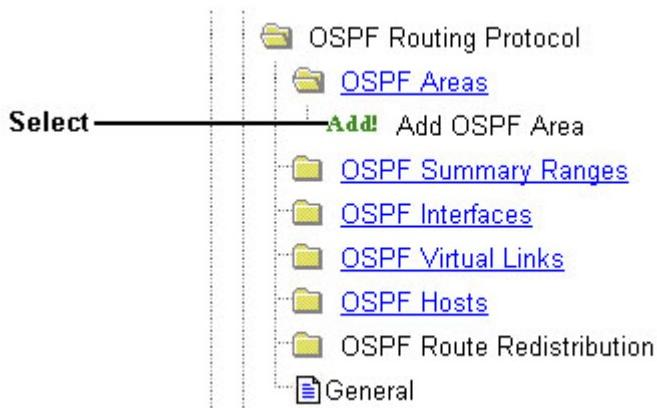
**OSPF Area Configuration**

Area Number (0-2)	0
Area ID	0.0.0.0
Enabled?	enabled
Area Type	transit
Stub Area Metric (1-65535)	1
SPF Interval (0-255)	10
Authentication Type?	none

**Submit**   **Delete**

- Click **Submit**.

d. Select **Add OSPF Area**.



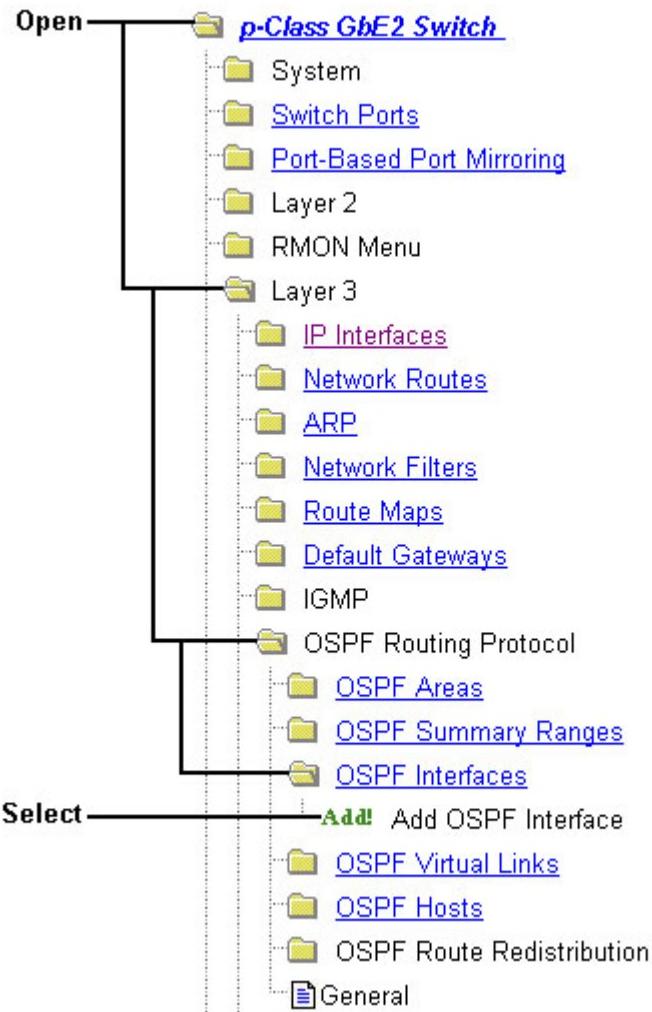
e. Configure the OSPF area 1.

**OSPF Area Configuration**

Area Number (0-2)	<input type="text" value="1"/>
Area ID	<input type="text" value="0.0.0.1"/>
Enabled?	<input type="button" value="enabled"/>
Area Type	<input type="button" value="stub"/>
Stub Area Metric (1-65535)	<input type="text" value="1"/>
SPF Interval (0-255)	<input type="text" value="10"/>
Authentication Type?	<input type="button" value="none"/>

f. Click **Submit**.

5. Configure OSPF Interfaces.
- Open the OSPF Interfaces folder, and select **Add OSPF Interface**.



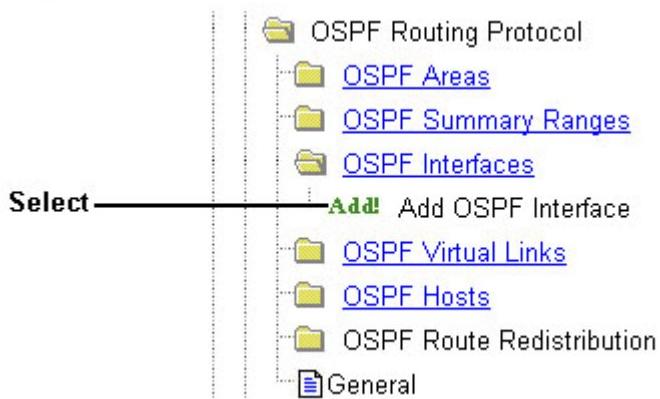
- b. Configure the OSPF Interface 1, and attach it to the backbone area 0.

### OSPF Interface Configuration

IP Interface Identifier (1-255)	<input type="text" value="1"/>
Area Number (0-2)	<input type="text" value="0"/>
Enabled?	<input type="button" value="enabled"/>
Router Priority (0-255)	<input type="text" value="1"/>
Output Cost (1-65535)	<input type="text" value="1"/>
Hello Interval (1-65535 sec)	<input type="text" value="10"/>
Dead Interval (1-65535 sec)	<input type="text" value="40"/>
Transit Delay (1-3600 sec)	<input type="text" value="1"/>
Retransmit Interval (1-3600 sec)	<input type="text" value="5"/>
Authentication Key	<input type="text"/>
MD5 Key ID (1-255)	<input type="text" value="0"/>

c. Click **Submit**.

d. Select **Add OSPF Interface**.



- e. Configure the OSPF Interface 2, and attach it to the stub area 1.

### OSPF Interface Configuration

IP Interface Identifier (1-255)	2
Area Number (0-2)	1
Enabled?	<input checked="" type="checkbox"/>
Router Priority (0-255)	1
Output Cost (1-65535)	1
Hello Interval (1-65535 sec)	10
Dead Interval (1-65535 sec)	40
Transit Delay (1-3600 sec)	1
Retransmit Interval (1-3600 sec)	5
Authentication Key	
MD5 Key ID (1-255)	0

f. Click **Submit**.

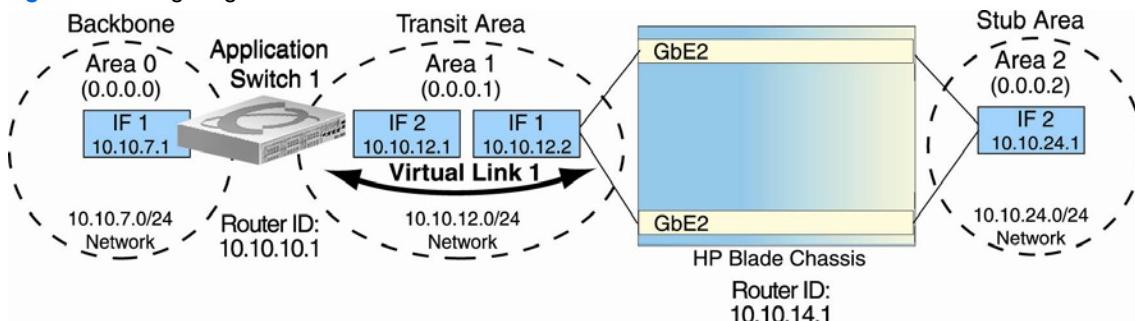
6. Apply, verify, and save the configuration.



## Example 2: Virtual links

In the example shown in the following figure, area 2 is not physically connected to the backbone as is usually required. Instead, area 2 will be connected to the backbone via a virtual link through area 1. The virtual link must be configured at each endpoint.

**Figure 22** Configuring a virtual link



## Configuring OSPF for a virtual link on Switch A

1. Configure IP interfaces on each network that will be attached to the switch.

In this example, two IP interfaces are needed on Switch A: one for the backbone network on 10.10.7.0/24 and one for the transit area network on 10.10.12.0/24.

```
>> # /cfg/l3/if 1          (Select menu for IP interface 1)
>> IP Interface 1 # addr 10.10.7.1  (Set IP address on backbone network)
>> IP Interface 1 # mask 255.255.255.0 (Set IP mask on backbone network)
>> IP Interface 1 # enable        (Enable IP interface 1)
>> IP Interface 1 # ../if 2      (Select menu for IP interface 2)
>> IP Interface 2 # addr 10.10.12.1 (Set IP address on
                                  transit area network)
>> IP Interface 2 # mask 255.255.255.0 (Set IP mask on
                                  transit area network)
>> IP Interface 2 # enable        (Enable interface 2)
```

2. Configure the router ID.

A router ID is required when configuring virtual links. Later, when configuring the other end of the virtual link on Switch B, the router ID specified here will be used as the target virtual neighbor (nbr) address

```
>> IP Interface 2 # /cfg/l3/rtrid 10.10.10.1          (Set static router ID)
```

3. Enable OSPF.

```
>> IP # /cfg/l3/ospf/on
```

4. Define the backbone.

```
>> Open Shortest Path First # aindex 0      (Select menu for area index 0)
>> OSPF Area (index) 0 # areaid 0.0.0.0    (Set the area ID)
>> OSPF Area (index) 0 # type transit     (Define backbone as transit type)
>> OSPF Area (index) 0 # enable           (Enable the area)
```

5. Define the transit area.

The area that contains the virtual link must be configured as a transit area

```
>> OSPF Area (index) 0 # ../aindex 1   (Select menu for area index 1)
>> OSPF Area (index) 1 # areaid 0.0.0.1 (Set the area ID for OSPF area 1)
>> OSPF Area (index) 1 # type transit  (Define area as transit type)
>> OSPF Area (index) 1 # enable       (Enable the area)
```

6. Attach the network interface to the backbone.

```
>> OSPF Area (index) 1 # ../if 1      (Select OSPF menu for IP interface 1)
>> OSPF Interface 1 # aindex 0      (Attach network to backbone index)
>> OSPF Interface 1 # enable        (Enable the backbone interface)
```

7. Attach the network interface to the transit area.

```
>> OSPF Interface 1 # ../if 2      (Select OSPF menu for IP interface 2)
>> OSPF Interface 2 # aindex 1      (Attach network to transit area index)
>> OSPF Interface 2 # enable        (Enable the transit area interface)
```

8. Configure the virtual link.

The nbr router ID configured in this step must be the same as the router ID that will be configured for Switch B in step 2.

```
>> OSPF Interface 2 # ../virt 1      (Specify a virtual link number)
>> OSPF Virtual Link 1 # aindex 1    (Specify the transit area
                                    for the virtual link)
>> OSPF Virtual Link 1 # nbr 10.10.14.1 (Specify the router ID
                                         of the recipient)
>> OSPF Virtual Link 1 # enable      (Enable the virtual link)
```

9. Apply and save the configuration changes

```
>> OSPF Interface 2 # apply        (Apply all changes)
>> OSPF Interface 2 # save         (Save all changes)
```

## Configuring OSPF for a virtual link on Switch B

1. Configure IP interfaces on each network that will be attached to OSPF areas.

Two IP interfaces are needed on Switch B: one for the transit area network on 10.10.12.0/24 and one for the stub area network on 10.10.24.0/24.

```
>> # /cfg/l3/if 1          (Select menu for IP interface 1)
>> IP Interface 1 # addr 10.10.12.2   (Set IP address
                                         on transit area network)
>> IP Interface 1 # mask 255.255.255.0 (Set IP mask
                                         on transit area network)
>> IP Interface 1 # enable           (Enable IP interface 1)
>> IP Interface 1 # ../if 2         (Select menu for IP interface 2)
>> IP Interface 2 # addr 10.10.24.1 (Set IP address on stub area network)
>> IP Interface 2 # mask 255.255.255.0 (Set IP mask on stub area network)
>> IP Interface 2 # enable           (Enable IP interface 2)
```

2. Configure the router ID.

A router ID is required when configuring virtual links. This router ID should be the same one specified as the target virtual neighbor (nbr) on Switch A.

```
>> IP Interface 2 # /cfg/l3/rtrid 10.10.14.1 (Set static router ID)
```

3. Enable OSPF.

```
>> IP# /cfg/l3/ospf/on
```

4. Define the backbone.

This version of GbE2 software requires that a backbone index be configured on the non-backbone end of the virtual link as follows:

```
>> Open Shortest Path First # aindex 0 (Select the menu for area index 0)
>> OSPF Area (index) 0 # areaid 0.0.0.0 (Set the area ID for OSPF area 0)
>> OSPF Area (index) 0 # enable        (Enable the area)
```

5. Define the transit area.

```
>> OSPF Area (index) 0 # ../aindex 1 (Select menu for area index 1)
>> OSPF Area (index) 1 # areaid 0.0.0.1 (Set the area ID for OSPF area 1)
>> OSPF Area (index) 1 # type transit (Define area as transit type)
>> OSPF Area (index) 1 # enable       (Enable the area)
```

6. Define the stub area.

```
>> OSPF Area (index) 1 # ../aindex 2 (Select the menu for area index 2)
>> OSPF Area (index) 2 # areaid 0.0.0.2 (Set the area ID for OSPF area 2)
>> OSPF Area (index) 2 # type stub    (Define area as stub type)
>> OSPF Area (index) 2 # enable      (Enable the area)
```

7. Attach the network interface to the backbone.

```
>> OSPF Area (index) 2 # ../if 1   (Select OSPF menu for IP interface 1)
>> OSPF Interface 1 # aindex 1    (Attach network to transit area index)
>> OSPF Interface 1 # enable     (Enable the transit area interface)
```

8. Attach the network interface to the transit area.

```
>> OSPF Interface 1 # ../if 2     (Select OSPF menu for IP interface 2)
>> OSPF Interface 2 # aindex 2    (Attach network to stub area index)
>> OSPF Interface 2 # enable     (Enable the stub area interface)
```

9. Configure the virtual link.

The nbr router ID configured in this step must be the same as the router ID that was configured for Switch A in step 2.

```
>> OSPF Interface 2 # ../virt 1      (Specify a virtual link number)
>> OSPF Virtual Link 1 # aindex 1    (Specify the transit area
                                         for the virtual link)
>> OSPF Virtual Link 1 # nbr 10.10.10.1 (Specify the router ID
                                         of the recipient)
>> OSPF Virtual Link 1 # enable      (Enable the virtual link)
```

10. Apply and save the configuration changes.

```
>> OSPF Interface 2 # apply        (Apply all changes)
>> OSPF Interface 2 # save         (Save all changes)
```

## Other Virtual Link Options

- You can use redundant paths by configuring multiple virtual links.
- Only the endpoints of the virtual link are configured. The virtual link path may traverse multiple routers in an area as long as there is a routable path between the endpoints.

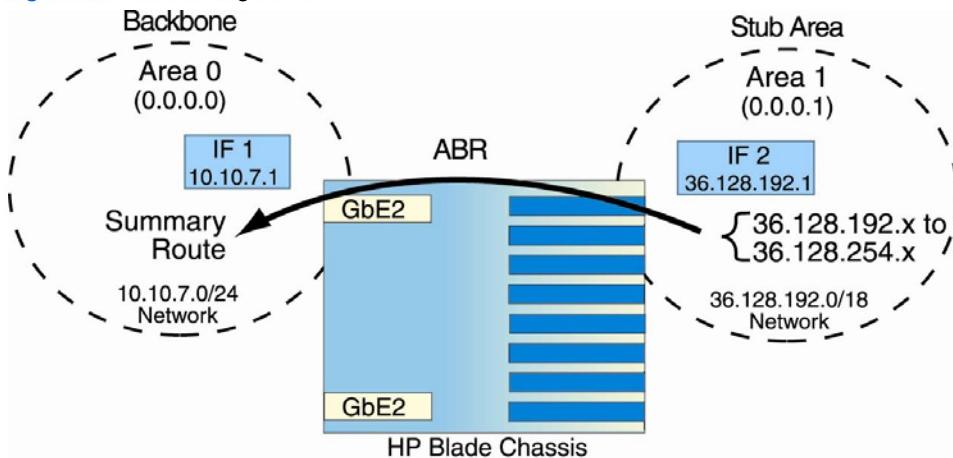
## Example 3: Summarizing routes

By default, ABRs advertise all the network addresses from one area into another area. Route summarization can be used for consolidating advertised addresses and reducing the perceived complexity of the network.

If the network IP addresses in an area are assigned to a contiguous subnet range, you can configure the ABR to advertise a single summary route that includes all the individual IP addresses within the area.

The following example shows one summary route from area 1 (stub area) injected into area 0 (the backbone). The summary route consists of all IP addresses from 36.128.192.0 through 36.128.254.255 except for the routes in the range 36.128.200.0 through 36.128.200.255

**Figure 23** Summarizing routes



**NOTE:** You can specify a range of addresses to prevent advertising by using the hide option. In this example, routes in the range 36.128.200.0 through 36.128.200.255 are kept private.

Follow this procedure to configure OSPF support on Switch A and Switch B, as shown in the figure.

1. Configure IP interfaces for each network which will be attached to OSPF areas.

```
>> # /cfg/l3/if 1          (Select menu for IP interface 1)
>> IP Interface 1 # addr 10.10.7.1 (Set IP address on backbone network)
>> IP Interface 1 # mask 255.255.255.0 (Set IP mask on backbone network)
>> IP Interface 1 # ena   (Enable IP interface 1)
>> IP Interface 1 # ../if 2 (Select menu for IP interface 2)
>> IP Interface 2 # addr 36.128.192.1 (Set IP address on stub area network)
>> IP Interface 2 # mask 255.255.192.0 (Set IP mask on stub area network)
>> IP Interface 2 # ena   (Enable IP interface 2)
```

2. Enable OSPF.

```
>> IP Interface 2 # /cfg/l3/ospf/on
```

3. Define the backbone.

```
>> Open Shortest Path First # aindex 0 (Select menu for area index 0)
>> OSPF Area (index) 0 # areaid 0.0.0.0 (Set the ID for backbone area 0)
>> OSPF Area (index) 0 # type transit (Define backbone as transit type)
>> OSPF Area (index) 0 # enable    (Enable the area)
```

**4.** Define the stub area.

```
>> OSPF Area (index) 0 # ../../aindex 1      (Select menu for area index 1)
>> OSPF Area (index) 1 # areaid 0.0.0.1     (Set the area ID for OSPF
                                              area 1)
>> OSPF Area (index) 1 # type stub          (Define area as stub type)
>> OSPF Area (index) 1 # enable             (Enable the area)
```

**5.** Attach the network interface to the backbone.

```
>> OSPF Area (index) 1 # ../../if 1        (Select OSPF menu for IP interface 1)
>> OSPF Interface 1 # aindex 0            (Attach network to backbone index)
>> OSPF Interface 1 # enable             (Enable the backbone interface)
```

**6.** Attach the network interface to the stub area.

```
>> OSPF Interface 1 # ../../if 2        (Select OSPF menu for IP interface 2)
>> OSPF Interface 2 # aindex 1          (Attach network to stub area index)
>> OSPF Interface 2 # enable           (Enable the stub area interface)
```

**7.** Configure route summarization by specifying the starting address and mask of the range of addresses to be summarized.

```
>> OSPF Interface 2 # ../../range 1    (Select menu for summary range)
>> OSPF Summary Range 1 # addr 36.128.192.0 (Set base IP address
                                              of summary range)
>> OSPF Summary Range 1 # mask 255.255.192.0 (Set mask address
                                              for summary range)
>> OSPF Summary Range 1 # aindex 0      (Inject summary route into backbone)
>> OSPF Summary Range 1 # enable       (Enable summary range)
```

**8.** Use the hide command to prevent a range of addresses from advertising to the backbone.

```
>> OSPF Interface 2 # ../../range 2    (Select menu for summary range)
>> OSPF Summary Range 2 # addr 36.128.200.0 (Set base IP address)
>> OSPF Summary Range 2 # mask 255.255.255.0 (Set mask address)
>> OSPF Summary Range 2 # hide enable   (Hide the range of addresses)
```

**9.** Apply and save the configuration changes.

```
>> OSPF Summary Range 2 # apply        (Apply all changes)
>> OSPF Summary Range 2 # save         (Save all changes)
```

## Verifying OSPF configuration

Use the following commands to verify the OSPF configuration on your switch:

- /info/l3/ospf/general
- /info/l3/ospf/nbr
- /info/l3/ospf/dbase/dbsum
- /info/l3/ospf/route
- /stats/l3/route

See the *HP ProLiant BL p-Class GbE2 Interconnect Switch Command Reference Guide* for information on the above commands.

# Remote monitoring

## Introduction

Remote Monitoring (RMON) allows network devices to exchange network monitoring data.

RMON performs the following major functions:

- Gathers cumulative statistics for Ethernet interfaces
- Tracks a history of statistics for Ethernet interfaces
- Creates and triggers alarms for user-defined events

## Overview

The RMON MIB provides an interface between the RMON agent on the HP ProLiant BL p-Class GbE2 Interconnect Switch and an RMON management application. The RMON MIB is described in RFC 1757.

The RMON standard defines objects that are suitable for the management of Ethernet networks. The RMON agent continuously collects statistics and proactively monitors switch performance. RMON allows you to monitor traffic flowing through the GbE2 Interconnect Switch.

The GbE2 Interconnect Switch supports the following RMON Groups, as described in RFC 1757:

- Group 1: Statistics
- Group 2: History
- Group 3: Alarms
- Group 9: Events

## RMON group 1—statistics

The GbE2 supports collection of Ethernet statistics as outlined in the RMON statistics MIB, in reference to etherStatsTable. You can enable RMON statistics on a per-port basis, and you can view them using the /stat/port x/rmon command. RMON statistics are sampled every second, and new data overwrites any old data on a given port.



**NOTE:** RMON port statistics must be enabled for the port before you can view RMON statistics.

## Configuring RMON group 1 (CLI example)

1. Enable RMON on each port where you wish to collect RMON statistics.

```
>> /cfg/port 23/rmon          (Select Port 23 RMON)
>> Port 23 RMON# ena         (Enable RMON)
>> Port 23 RMON# apply       (Make your changes active)
>> Port 23 RMON# save       (Save for restore after
reboot)
```

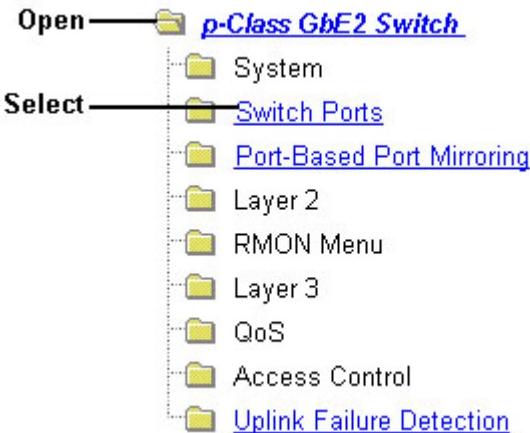
2. View RMON statistics for the port.

```
>> /stats/port 23                                     (Select Port 23 Stats)
>> Port Statistics# rmon

-----
RMON statistics for port 23:
etherStatsDropEvents:                               NA
etherStatsOctets:                                  7305626
etherStatsPkts:                                    48686
etherStatsBroadcastPkts:                           4380
etherStatsMulticastPkts:                           6612
etherStatsCRCAlignErrors:                          22
etherStatsUndersizePkts:                           0
etherStatsOversizePkts:                           0
etherStatsFragments:                             2
etherStatsJabbers:                                0
etherStatsCollisions:                            0
etherStatsPkts64Octets:                           27445
etherStatsPkts65to127Octets:                      12253
etherStatsPkts128to255Octets:                     1046
etherStatsPkts256to511Octets:                     619
etherStatsPkts512to1023Octets:                    7283
etherStatsPkts1024to1518Octets:                   38
```

## Configuring RMON group 1 (BBI example)

1. Configure ports.
  - a. Click the **Configure** context button.
  - b. Select **Switch Ports** (click the underlined text, not the folder).



2. Select a port.

Switch Ports Configuration								
Switch Port	State	VLAN Tagging	Default PVID	Multicast Threshold	Broadcast Threshold	Destination Lookup Fail Threshold	802.1p Priority	
<a href="#">1</a>	enabled	disabled	1	disabled	disabled	disabled	0	
<a href="#">2</a>	enabled	disabled	1	disabled	disabled	disabled	0	
<a href="#">3</a>	enabled	disabled	1	disabled	disabled	disabled	0	
<a href="#">4</a>	enabled	disabled	1	disabled	disabled	disabled	0	
<a href="#">5</a>	enabled	disabled	1	disabled	disabled	disabled	0	
<a href="#">6</a>	enabled	disabled	1	disabled	disabled	disabled	0	
<a href="#">7</a>	enabled	disabled	1	disabled	disabled	disabled	0	
<a href="#">8</a>	enabled	disabled	1	disabled	disabled	disabled	0	
<a href="#">9</a>	enabled	disabled	1	disabled	disabled	disabled	0	
<a href="#">10</a>	enabled	disabled	1	disabled	disabled	disabled	0	
⋮								
<a href="#">22</a>	enabled	disabled	100	disabled	disabled	disabled	0	
<b>Select</b> <a href="#">23</a>	enabled	disabled	4095	disabled	disabled	disabled	0	
<a href="#">24</a>	enabled	disabled	134	disabled	disabled	disabled	0	

3. Enable RMON on the port.

### Switch Port 23 Configuration

Switch Port State	Enabled <input type="button" value="▼"/>
RMON Instrumentation	Enabled <input type="button" value="▼"/>
VLAN Tagging	Disabled <input type="button" value="▼"/>
PVID Tagging	Enabled <input type="button" value="▼"/>
Port STP	On <input type="button" value="▼"/>
Default Port VLAN ID (1 - 4095)	1
⋮	
<input type="button" value="Submit"/>	

4. Click Submit.

5. Apply, verify, and save the configuration.



## RMON group 2—history

The RMON History group allows you to sample and archive Ethernet statistics for a specific interface during a specific time interval.



**NOTE:** RMON port statistics must be enabled for the port before an RMON history group can monitor the port.

Data is stored in **buckets**, which store data gathered during discreet sampling intervals. At each configured interval, the history instance takes a sample of the current Ethernet statistics, and places them into a bucket. History data buckets reside in dynamic memory. When the switch is re-booted, the buckets are emptied.

Requested buckets (/cfg/rmon/hist x/rbnum) are the number of buckets, or data slots, requested by the user for each History Group. Granted buckets (/info/rmon/hist x/Gbnum) are the number of buckets granted by the system, based on the amount of system memory available. The system grants a maximum of 50 buckets.

Use an SNMP browser to view History samples.

### History MIB objects

The type of data that can be sampled must be of an ifIndex object type, as described in RFC1213 and RFC1573. The most common data type for the history sample is as follows:

```
1.3.6.1.2.1.2.2.1.1.x -mgmt.interfaces.ifTable.ifIndex.interface
```

The last digit (x) represents the interface on which to monitor, which corresponds to the port number (1-24). History sampling is done per port, by utilizing the interface number to specify the port number.

### Configure RMON group 2 (CLI example)

1. Enable RMON on each port where you wish to collect RMON History.

>> /cfg/port 23/rmon	(Select Port 23 RMON)
>> Port 23# ena	(Enable RMON)
>> Port 23 RMON# apply	(Make your changes active)
>> Port 23 RMON# save	(Save for restore after reboot)

2. Configure the RMON History parameters.

>> /cfg/rmon/hist 1	(Select RMON History 1)
>> RMON History 1# ifoid 1.3.6.1.2.1.2.2.1.1.23	
>> RMON History 1# rbnum 30	
>> RMON History 1# intrval 120	
>> RMON History 1# owner "Owner_History_1"	

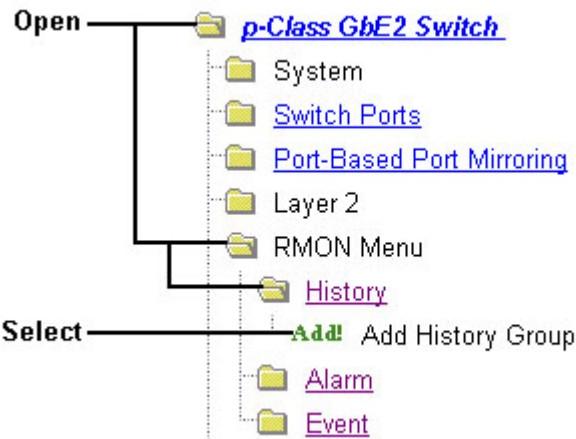
3. Apply and save the configuration.

>> RMON History 1# apply	(Make your changes active)
>> RMON History 1# save	(Save for restore after reboot)

This configuration creates an RMON History group to monitor port 23. It takes a data sample every two minutes, and places the data into one of the 30 requested buckets. After 30 samples are gathered, the new samples overwrite the previous samples, beginning with the first bucket. Use SNMP to view the data.

## Configure RMON group 2 (BBI example)

1. Configure an RMON History group.
  - a. Click the **Configure** context button.
  - b. Open the Switch folder, and select RMON > History > **Add History Group**.



2. Configure RMON History Group parameters.

RMON History Configuration	
History Group ID (1 - 65535)	1
MIB Object ID	1.3.6.1.2.1.2.2.1.1.23
Number of Buckets Requested (1 - 65535)	30
Polling Interval (1 - 3600)	1800
Owner	Owner_History_1

Submit    Delete

3. Click **Submit**.
4. Apply, verify, and save the configuration.



## RMON group 3—alarms

The RMON Alarm group allows you to define a set of thresholds used to determine network performance. When a configured threshold is crossed, an alarm is generated. For example, you can configure the switch to issue an alarm if more than 1,000 CRC errors occur during a 10-minute time interval.

Each Alarm index consists of a variable to monitor, a sampling time interval, and parameters for rising and falling thresholds. The Alarm group can be used to track rising or falling values for a MIB object. The object must be a counter, gauge, integer, or time interval.

Use the `/cfg/rmon/alarm x/revtidx` or `/fevtidx` to correlate an alarm index to an event index. When the alarm threshold is reached, the corresponding event is triggered.

## Alarm MIB objects

The most common data types used for alarm monitoring are ifStats: errors, drops, bad CRCs, and so on. These MIB Object Identifiers (OIDs) correlate to the ones tracked by the History group. An example of an ICMP stat is as follows:

1.3.6.1.2.1.5.1.0 - mgmt.icmp.icmpInMsgs

The last digit (x) represents the interface on which to monitor, which corresponds to the interface number, or port number, as follows:

1-256 = IF 1-256  
257 = port 1  
258 = port 2  
...  
280 = port 24

This value represents the alarm's MIB OID, as a string. Note that for non-tables, you must supply a .0 to specify end node.

### Configure RMON group 3 (CLI example 1)

1. Configure the RMON Alarm parameters to track the number of packets received on a port.

```
>> /cfg/rmon/alarm 6                                (Select RMON Alarm 6)
>> RMON Alarm 6# oid 1.3.6.1.2.1.2.1.10.275
>> RMON Alarm 6# intrval 3600
>> RMON Alarm 6# almttype rising
>> RMON Alarm 6# rlimit 2000000000
>> RMON Alarm 6# revtidx 6
>> RMON Alarm 6# sample abs
>> RMON Alarm 6# owner "Alarm_for_ifInOctets"
```

2. Apply and save the configuration.

```
>> RMON Alarm 6# apply                            (Make your changes active)
>> RMON Alarm 6# save                            (Save for restore after reboot)
```

This configuration creates an RMON alarm that checks ifInOctets on port 19 once every hour. If the statistic exceeds two billion, an alarm is generated that triggers event index 6.

### Configure RMON group 3 (CLI example 2)

1. Configure the RMON Alarm parameters to track ICMP messages.

```
>> /cfg/rmon/alarm 5                                (Select RMON Alarm 5)
>> RMON Alarm 5# oid 1.3.6.1.2.1.5.8.0
>> RMON Alarm 5# intrval 60
>> RMON Alarm 5# almttype rising
>> RMON Alarm 5# rlimit 200
>> RMON Alarm 5# revtidx 5
>> RMON Alarm 5# sample delta
>> RMON Alarm 5# owner "Alarm_for_icmpInEchos"
```

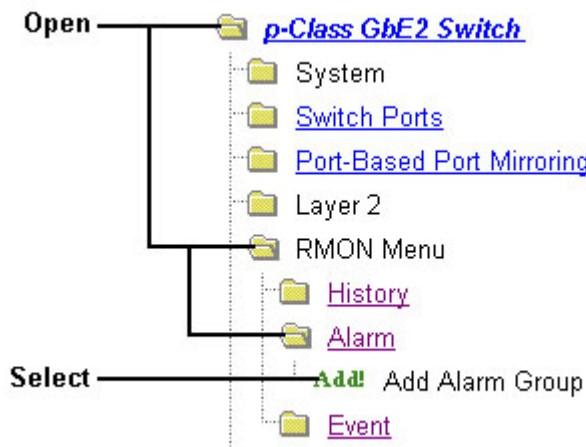
2. Apply and save the configuration.

```
>> RMON Alarm 5# apply                            (Make your changes active)
>> RMON Alarm 5# save                            (Save for restore after reboot)
```

This configuration creates an RMON alarm that checks icmpInEchos on the switch once every minute. If the statistic exceeds 200 within a 60 second interval, an alarm is generated that triggers event index 5.

## Configure RMON group 3 (BBI example 1)

1. Configure an RMON Alarm group.
  - a. Click the **Configure** context button.
  - b. Open the Switch folder, and select RMON > Alarm > **Add Alarm Group**.



2. Configure RMON Alarm Group parameters to check `ifInOctets` on port 19 once every hour. Enter a rising limit of two billion, and a rising event index of 6. This configuration creates an RMON alarm that checks `ifInOctets` on port 19 once every hour. If the statistic exceeds two billion, an alarm is generated that triggers event index 6.

RMON Alarm Configuration	
Alarm Group ID (1 - 65535)	6
MIB Object ID	1.3.6.1.2.1.2.2.1.10.275
Rising Limit (-2147483647 - 2147483647)	20000000000
Falling Limit (-2147483647 - 2147483647)	0
Rising Event Index (0 - 65535)	6
Falling Event Index (0 - 65535)	0
Alarm Type	Rising ▾
Sample Type	Absolute ▾
Polling Interval (1 - 65535)	3600
Owner	Alarm_for_ifInOctets
 Submit    Delete	

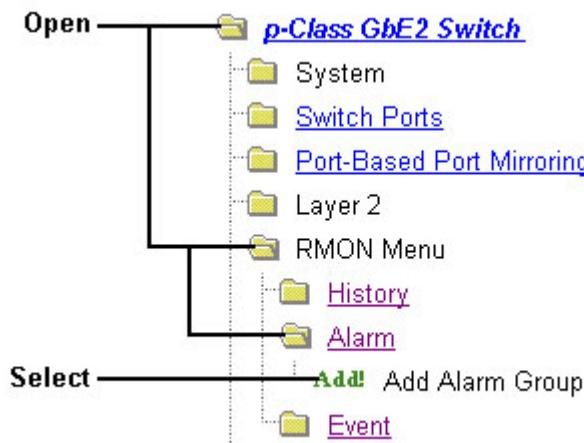
3. Click **Submit**.

4. Apply, verify, and save the configuration.



### Configure RMON group 3 (BBI example 2)

1. Configure an RMON Alarm group.
  - a. Click the **Configure** context button.
  - b. Open the Switch folder, and select RMON > Alarm > **Add Alarm Group**.



2. Configure RMON Alarm Group parameters to check `icmpInEchos`, with a polling interval of 60, a rising limit of 200, and a rising event index of 5. This configuration creates an RMON alarm that checks `icmpInEchos` on the switch once every minute. If the statistic exceeds 200 within a 60 second interval, an alarm is generated that triggers event index 5.

RMON Alarm Configuration	
Alarm Group ID (1 - 65535)	5
MIB Object ID	1.3.6.1.2.1.5.8.0
Rising Limit (-2147483647 - 2147483647)	200
Falling Limit (-2147483647 - 2147483647)	0
Rising Event Index (0 - 65535)	5
Falling Event Index (0 - 65535)	0
Alarm Type	Rising ▾
Sample Type	Delta ▾
Polling Interval (1 - 65535)	60
Owner	Alarm_for_icmpInEchos
<input type="button" value="Submit"/> <input type="button" value="Delete"/>	

3. Click **Submit**.

4. Apply, verify, and save the configuration.



## RMON group 9—events

The RMON Event group allows you to define events that are triggered by alarms. An event can be a log message, an SNMP trap message, or both.

When an alarm is generated, it triggers a corresponding event notification. Use the `/cfg/rmon/alarm x/revtidx` and `/fevtidx` commands to correlate an event index to an alarm.

RMON events use SNMP and SYSLOGs to send notifications. Therefore, an SNMP host (`/cfg/sys/snmp`) must be configured for trap event notification to work properly.

RMON uses a SYSLOG host to send syslog messages. Therefore, an existing SYSLOG host (`/cfg/sys/syslog`) must be configured for event log notification to work properly. Each log event generates a SYSLOG of type RMON that corresponds to the event.

## Configuring RMON group 9 (CLI example)

1. Configure the RMON Event parameters.

```
>> /cfg/rmon/event 5                                     (Select RMON Event 5)
>> RMON Event 5# descrn "SYSLOG_generation_event"
>> RMON Event 5# type log
>> RMON Event 5# owner "Owner_event_5"
```

2. Apply and save the configuration.

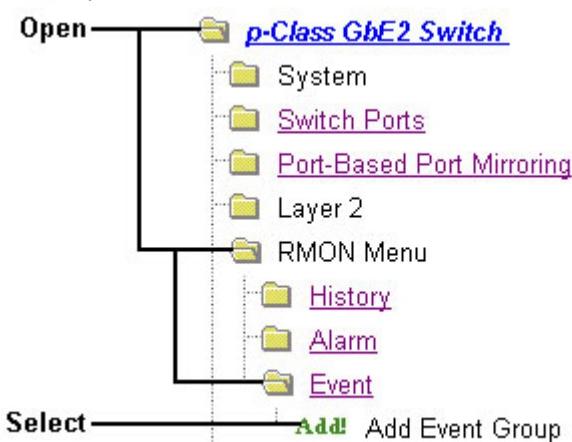
<pre>&gt;&gt; RMON Alarm 5# apply</pre>	(Make your changes active)
<pre>&gt;&gt; RMON Alarm 5# save</pre>	(Save for restore after reboot)

This configuration creates an RMON event that sends a SYSLOG message each time it is triggered by an alarm.

## Configuring RMON group 9 (BBI example 1)

1. Configure an RMON Event group.

- a. Click the **Configure** context button.
- b. Open the Switch folder, and select RMON > Event > **Add Event Group**.



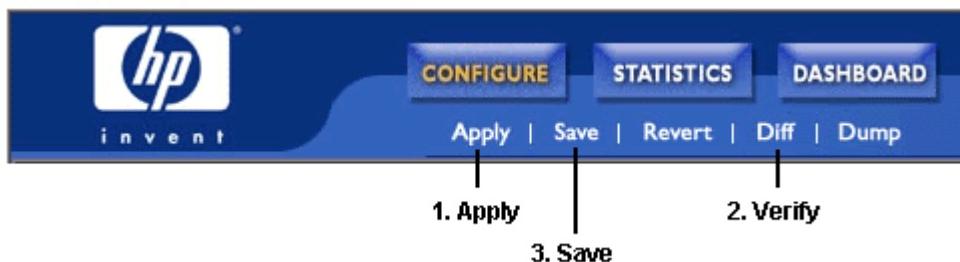
2. Configure RMON Event Group parameters. This configuration creates an RMON event that sends a SYSLOG message each time it is triggered by an alarm.

**RMON Event Configuration**

Event Group ID (1 - 65535)	5
Event Type	Log
Description	SYSLOG_generation_event
Owner	Owner_event_5

**Submit**   **Delete**

3. Click **Submit**.  
4. Apply, verify, and save the configuration.



# High availability

## Introduction

GbE2 Interconnect Switches support high availability network topologies. This release provides information about Uplink Failure Detection and Virtual Router Redundancy Protocol (VRRP).

## Uplink Failure Detection

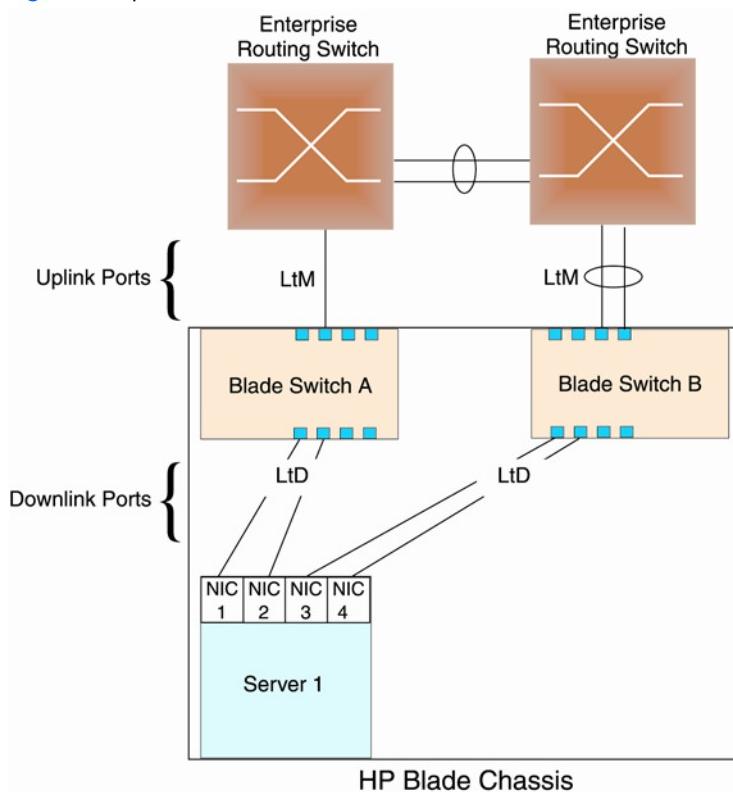
Uplink Failure Detection (UFD) is designed to support Network Adapter Teaming on HP server blades. For details about Network Adapter Teaming on HP ProLiant server blades, see the white paper at the following location:  
<http://h18004.www1.hp.com/products/servers/networking/whitepapers.html>

UFD allows the switch to monitor specific uplink ports to detect link failures. When the switch detects a link failure, it automatically disables specific downlink ports. The corresponding server's network adapter can detect the disabled downlink, and trigger a network-adapter failover to another port on the switch, or another switch in the chassis.

The switch automatically enables the downlink ports when the uplink returns to service.

The following figure shows a basic UFD configuration, with a Failure Detection Pair (FDP) that consists of one LtM (Link to Monitor) and one LtD (Link to Disable). When the switch detects a link failure in the LtM, it disables the ports in the LtD. The server blade detects the disabled downlink port, which triggers a NIC failover.

**Figure 24** Uplink Failure Detection for GbE2 Interconnect Switches



## Failure Detection Pair

To use UFD, you must configure a Failure Detection Pair and then turn UFD on. A Failure Detection Pair consists of the following groups of ports:

- **Link to Monitor (LtM)**

The Link to Monitor group consists of one uplink port (19-24), or one trunk group that contains only uplink ports. The switch monitors the LtM for link failure.

- **Link to Disable (LtD)**

The Link to Disable group consists of one or more downlink ports (1-16) and trunk groups that contain only downlink ports. When the switch detects a link failure on the LtM, it automatically disables all ports in the LtD.

When the LtM returns to service, the switch automatically enables all ports in the LtD.

## Spanning Tree Protocol with UFD

If Spanning Tree Protocol (STP) is enabled on ports in the LtM, then the switch monitors the STP state and the link status on ports in the LtM. The switch automatically disables the ports in the LtD when it detects a link failure or STP Blocking state.

When the switch determines that ports in the LtM are in STP Forwarding State, then it automatically enables the ports in the LtD, to fall back to normal operation.

## Configuration guidelines

This section provides important information about configuring UFD:

- UFD is required only when uplink-path redundancy is not available on the blade switches.
- Only one Failure Detection pair (one group of Links to Monitor and one group of Links to Disable) is supported on each switch (all VLANs and Spanning Tree Groups).
- An LtM can be either one uplink port or one Multi-Link trunk group of uplink ports.
- Ports that are already members of a trunk group are not allowed to be assigned to an LtM.
- A trunk group configured as an LtM can contain multiple uplink ports (19-24), but no downlink ports (1-16) or interconnect ports (17-18).
- An uplink port cannot be added to a trunk group if it already belongs to an LtM.
- An LtD can contain one or more ports, and/or one or more trunks
- A trunk group configured as an LtD can contain multiple downlink ports (1-16), but no uplink ports (19-24) or interconnect ports (17-18).

## Monitoring Uplink Failure Detection

The UFD information menu displays the current status of the LtM and LtD, and their member ports or trunks. For example:

```
>> Information# ufd
Uplink Failure Detection: Enabled
LtM status: Down
Member      STG      STG State        Link Status
-----      ---      -----          -----
port 24          1      DISABLED          down
                  10     DISABLED *
                  16     DISABLED *
* = STP turned off for this port.

LtD status: Auto Disabled
Member      Link Status
-----      -----
port 1       disabled
port 2       disabled
port 3       disabled
port 4       disabled
```

Use the /stats/ufd command to find out how many times link failure was detected on the LtM, how many times Spanning Tree blocking state was detected on the LtM, and how many times UFD disabled ports in the LtD.

## Configuring Uplink Failure Detection

The preceding figure shows a basic UFD configuration. Port 21 on Blade Switch A is connected to a Layer 2/3 routing switch outside of the chassis. Port 19 and port 20 on Blade Switch B form a trunk that is connected to a different Layer 2/3 routing switch. The interconnect ports (17-18) are disabled.

In this example, NIC 1 is the primary network adapter, NIC 2, NIC 3, and NIC 4 are non-primary adapters. NIC 1 and NIC 2 are connected to port 1 and port 2 on Blade Switch A. NIC 3 and NIC 4 are connected to port 1 and port 2 on Blade Switch B.

### Configuring UFD on Switch A (CLI example)

1. Assign uplink ports (19-24) to be monitored for communication failure.

```
>> Main# /cfg/ufd/fdp ena          (Enable Failure Detection Pair)  
>> FDP# ltm                      (Select Link to Monitor menu)  
>> Failure Link to Monitor# addport 21 (Monitor uplink port 21)
```

2. Assign downlink ports (1-16) to disable when an uplink failure occurs.

```
>> /cfg/ufd/fdp/ltd             (Select Link to Disable menu)  
>> Failure Link to Disable# addport 1 (Add port 1 as a Link to Disable)  
>> Failure Link to Disable# addport 2 (Add port 2 as a Link to Disable)
```

3. Turn UFD on.

```
>> /cfg/ufd/on                  (Turn Uplink Failure Detection on)  
>> Uplink Failure Detection# apply (Make your changes active)  
>> Uplink Failure Detection# save (Save for restore after reboot)
```

When a link failure or Spanning Tree blocking occurs on port 21, Switch A disables port 1 and port 2.

### Configuring UFD on Switch B (CLI example)

1. Create a trunk group of uplink ports (19-24) to monitor. First you must set each port to full duplex mode.

```
>> Main# /cfg/port 19/gig	mode full      (Set port 19 to full duplex)  
>> Main# /cfg/port 20/gig	mode full      (Set port 20 to full duplex)  
>> Main# /cfg/trunk 2                (Create trunk group 2)  
>> Trunk group 2# ena              (Enable trunk group 2)  
>> Trunk group 2# add 19           (Add port 19 to trunk group 2)  
>> Trunk group 2# add 20           (Add port 20 to trunk group 2)
```

2. Assign the trunk group to be monitored for communication failure.

```
>> Main# /cfg/ufd/fdp ena          (Enable Failover Pair)  
>> FDP# ltm                      (Select Link to Monitor menu)  
>> Failover Link to Monitor# addtrnk 2 (Monitor trunk group 2)
```

3. Assign downlink ports (1-16) to disable when an uplink failure occurs.

```
>> Main# /cfg/ufd/fdp/ltd         (Select Link to Disable menu)  
>> Failover Link to Disable# addport 1 (Add port 1 as a Link to Disable)  
>> Failover Link to Disable# addport 2 (Add port 2 as a Link to Disable)
```

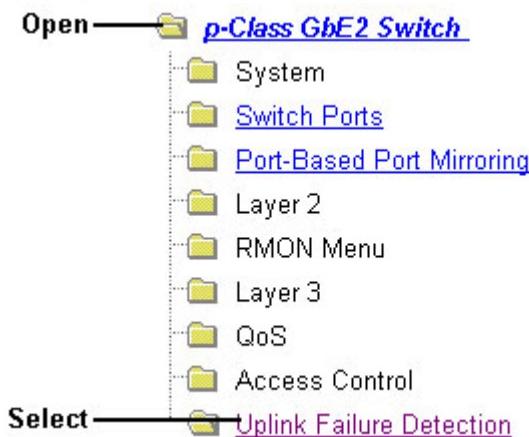
4. Turn UFD on.

```
>> Main# /cfg/ufd/on          (Turn Uplink Failure Detection on)
>> Uplink Failure Detection# apply (Make your changes active)
>> Uplink Failure Detection# save (Save for restore after reboot)
```

When a link failure or Spanning Tree blocking occurs on trunk group 2, Switch B disables port 1 and port 2.

## Configuring Uplink Failure Detection (BBI example)

1. Configure Uplink Failure Detection.
  - a. Click the **Configure** context button.
  - b. Open the Switch folder, and select **Uplink Failure Detection** (click the underlined text, not the folder).

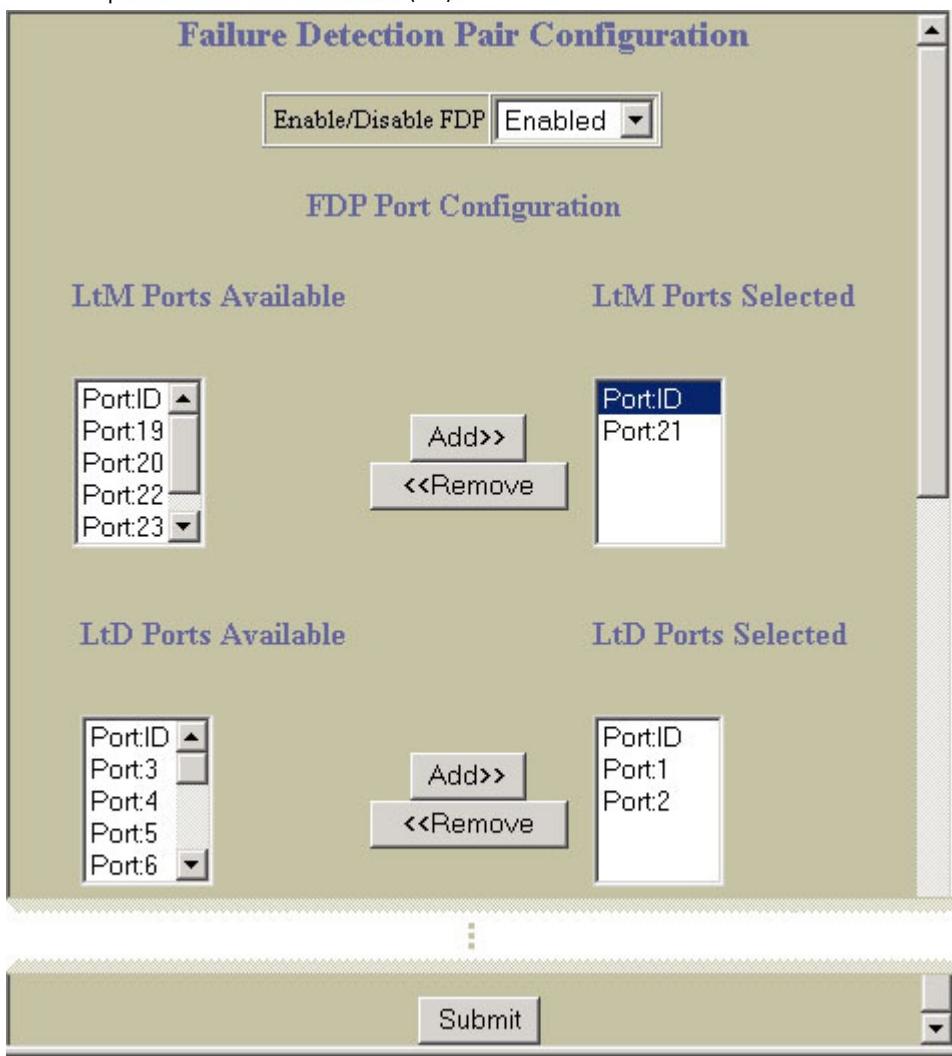


- c. Turn Uplink Failure Detection on, and then select FDP.

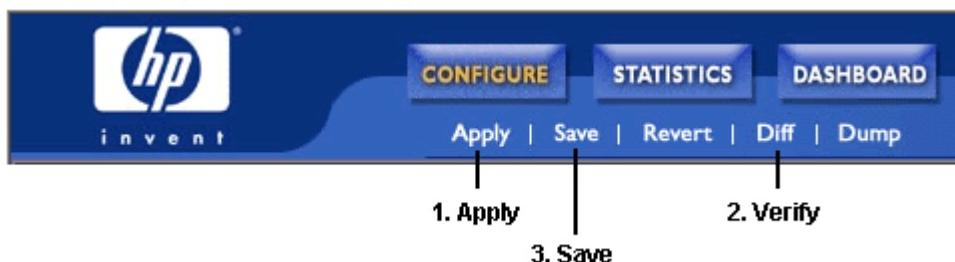
The dialog box has the title "Uplink Failure Detection Configuration". It contains the following fields:

- UFD state: A dropdown menu set to "ON".
- Submit: A button to submit the configuration.
- FDP: A link to access the Forwarding Database Page.

- d. Enable the FDP. Select ports in the LtM Ports Available list, and click **Add** to place the ports into the Link to Monitor (LtM). Select ports in the LtD Ports Available list, and click **Add** to place the ports into the Link to Disable (LtD).



- e. Click **Submit**.  
 2. Apply, verify, and save the configuration.



# VRRP overview

In a high-availability network topology, no device can create a single point-of-failure for the network or force a single point-of-failure to any other part of the network. This means that your network will remain in service despite the failure of any single device. To achieve this usually requires redundancy for all vital network components.

VRRP enables redundant router configurations within a LAN, providing alternate router paths for a host to eliminate single points-of-failure within a network. Each participating VRRP-capable routing device is configured with the same virtual router IP address and ID number. One of the virtual routers is elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will take control of the virtual router IP address and actively process traffic addressed to it.

With VRRP, Virtual Interface Routers (VIR) allows two VRRP routers to share an IP interface across the routers. VIRs provide a single Destination IP (DIP) for upstream routers to reach various servers, and provide a virtual default Gateway for the server blades.

## VRRP components

Each physical router running VRRP is known as a *VRRP router*.

### Virtual router

Two or more VRRP routers can be configured to form a *virtual router* (RFC 2338). Each VRRP router may participate in one or more virtual routers. Each virtual router consists of a user-configured *virtual router identifier* (VRID) and an IP address.

### Virtual router MAC address

The VRID is used to build the *virtual router MAC Address*. The five highest-order octets of the virtual router MAC Address are the standard MAC prefix (00-00-5E-00-01) defined in RFC 2338. The VRID is used to form the lowest-order octet.

### Owners and renters

Only one of the VRRP routers in a virtual router may be configured as the IP address owner. This router has the virtual router's IP address as its real interface address. This router responds to packets addressed to the virtual router's IP address for ICMP pings, TCP connections, and so on.

There is no requirement for any VRRP router to be the IP address owner. Most VRRP installations choose not to implement an IP address owner. For the purposes of this chapter, VRRP routers that are not the IP address owner are called *renters*.

### Master and backup virtual router

Within each virtual router, one VRRP router is selected to be the virtual router master. See "Selecting the Master VRRP Router" for an explanation of the selection process.



**NOTE:** If the IP address owner is available, it will always become the virtual router master.

The virtual router master forwards packets sent to the virtual router. It also responds to Address Resolution Protocol (ARP) requests sent to the virtual router's IP address. Finally, the virtual router master sends out periodic advertisements to let other VRRP routers know it is alive and its priority.

Within a virtual router, the VRRP routers not selected to be the master are known as virtual router backups. Should the virtual router master fail, one of the virtual router backups becomes the master and assumes its responsibilities.

### Virtual Interface Router

At Layer 3, a Virtual Interface Router (VIR) allows two VRRP routers to share an IP interface across the routers. VIRs provide a single Destination IP (DIP) for upstream routers to reach various destination networks, and provide a virtual default Gateway.



**NOTE:** Every VIR must be assigned to an IP interface, and every IP interface must be assigned to a VLAN. If no port in a VLAN has link up, the IP interface of that VLAN is down, and if the IP interface of a VIR is down, that VIR goes into INIT state.

# VRRP operation

Only the virtual router master responds to ARP requests. Therefore, the upstream routers only forward packets destined to the master. The master also responds to ICMP ping requests. The backup does not forward any traffic, nor does it respond to ARP requests.

If the master is not available, the backup becomes the master and takes over responsibility for packet forwarding and responding to ARP requests.

## Selecting the master VRRP router

Each VRRP router is configured with a priority between 1–254. A bidding process determines which VRRP router is or becomes the master—the VRRP router with the highest priority.

The master periodically sends advertisements to an IP multicast address. As long as the backups receive these advertisements, they remain in the backup state. If a backup does not receive an advertisement for three advertisement intervals, it initiates a bidding process to determine which VRRP router has the highest priority and takes over as master.

If, at any time, a backup determines that it has higher priority than the current master does, it can preempt the master and become the master itself, unless configured not to do so. In preemption, the backup assumes the role of master and begins to send its own advertisements. The current master sees that the backup has higher priority and will stop functioning as the master.

A backup router can stop receiving advertisements for one of two reasons—the master can be down, or all communications links between the master and the backup can be down. If the master has failed, it is clearly desirable for the backup (or one of the backups, if there is more than one) to become the master.



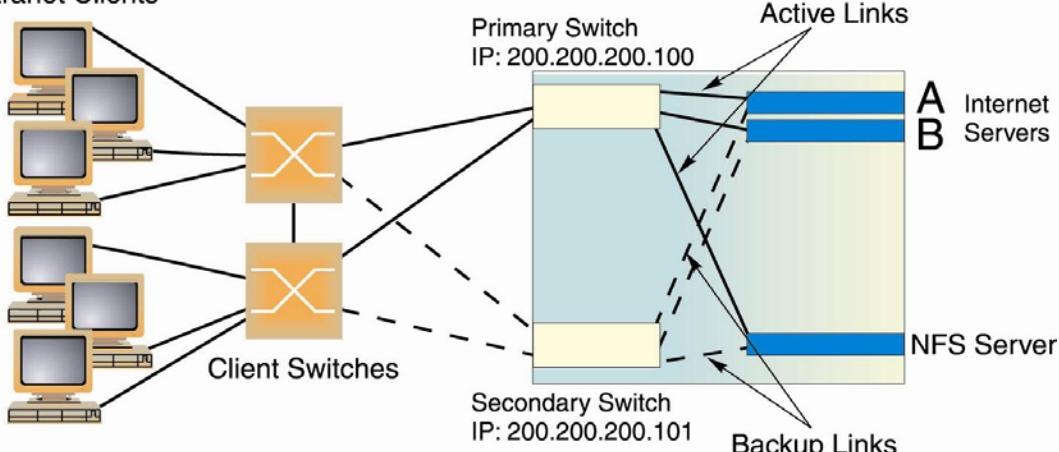
**NOTE:** If the master is healthy but communication between the master and the backup has failed, there will then be two masters within the virtual router. To prevent this from happening, configure redundant links to be used between the switches that form a virtual router.

## Failover methods

With service availability becoming a major concern on the Internet, service providers are increasingly deploying Internet traffic control devices, such as application switches, in redundant configurations. Traditionally, these configurations have been *hot-standby* configurations, where one switch is active and the other is in a standby mode. A non-VRRP hot-standby configuration is shown in the figure below:

**Figure 25** Non-VRRP hot-standby configuration

Intranet Clients



While hot-standby configurations increase site availability by removing single points-of-failure, service providers increasingly view them as an inefficient use of network resources because one functional application switch sits by idly until a failure calls it into action. Service providers now demand that vendors' equipment support redundant configurations where all devices can process traffic when they are healthy, increasing site throughput and decreasing user response times when no device has failed.

GbE2 high availability configurations are based on VRRP. The GbE2 software implementation of VRRP includes proprietary extensions.

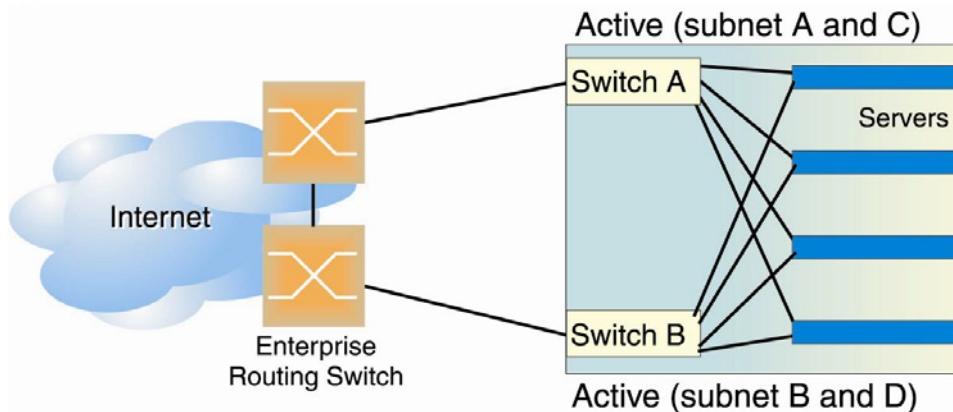
The GbE2 software implementation of VRRP supports the Active-Active mode of high availability.

## Active-Active redundancy

In an active-active configuration, shown in the following figure, two switches provide redundancy for each other, with both active at the same time. Each switch processes traffic on a different subnet. When a failure occurs, the remaining switch can process traffic on all subnets.

The following figure shows an Active-Active configuration example.

**Figure 26** Active-Active redundancy



## GbE2 extensions to VRRP

This section describes VRRP enhancements that are implemented in GbE2 software:

### Tracking VRRP router priority

GbE2 software supports a tracking function that dynamically modifies the priority of a VRRP router, based on its current state. The objective of tracking is to have, whenever possible, the master bidding processes for various virtual routers in a LAN converge on the same switch. Tracking ensures that the selected switch is the one that offers optimal network performance. For tracking to have any effect on virtual router operation, preemption must be enabled.

GbE2 software can track the attributes listed in the following table:

**Table 20** VRRP tracking parameters

Parameter	Description
/cfg/13/vrrp/track/ifs	Number of IP interfaces on the switch that are active ("up") Helps elect the virtual routers with the most available routes as the master. (An IP interface is considered active when there is at least one active port on the same VLAN.) This parameter influences the VRRP router's priority in virtual interface routers.
/cfg/13/vrrp/track/ports	Number of active ports on the same VLAN Helps elect the virtual routers with the most available ports as the master. This parameter influences the VRRP router's priority in virtual interface routers.
/cfg/13/vrrp/track/vr	Number of virtual routers in master mode on the switch Useful for ensuring that traffic for any particular client/ server pair is handled by the same switch, increasing routing efficiency. This parameter influences the VRRP router's priority in virtual interface routers.

Each tracked parameter has a user-configurable weight associated with it. As the count associated with each tracked item increases (or decreases), so does the VRRP router's priority, subject to the weighting associated with each tracked item. If the priority level of a standby is greater than that of the current master, then the standby can assume the role of the master.

See "Configuring the Switch for Tracking" for an example on how to configure the switch for tracking VRRP priority.

# Virtual router deployment considerations

Review the following issues described in this section to prevent network problems when deploying virtual routers:

- Assigning VRRP Virtual Router ID
- Configuring the Switch for Tracking

## Assigning VRRP virtual router ID

During the software upgrade process, VRRP virtual router IDs are assigned automatically if failover is enabled on the switch. When configuring virtual routers at any point after upgrade, virtual router ID numbers (/cfg/13/vrrp/vr #/vrid) must be assigned. The virtual router ID may be configured as any number between 1 and 255.

## Configuring the switch for tracking

Tracking configuration largely depends on user preferences and network environment. Consider the configuration shown in the previous figure. Assume the following behavior on the network:

- Switch A is the master router upon initialization.
- If Switch A is the master and it has one fewer active servers than Switch B, then Switch A remains the master.
- This behavior is preferred because running one server down is less disruptive than bringing a new master online and severing all active connections in the process.
- If Switch A is the master and it has two or more active servers fewer than Switch B, then Switch B becomes the master.
- If Switch B is the master, it remains the master even if servers are restored on Switch A such that it has one fewer or an equal number of servers.
- If Switch B is the master and it has one active server fewer than Switch A, then Switch A becomes the master.

The user can implement this behavior by configuring the switch for tracking as follows:

1. Set the priority for Switch A to 101.
2. Leave the priority for Switch B at the default value of 100.
3. On both switches, enable tracking based on ports (ports), interfaces (ifs), or virtual routers (vr). You can choose any combination of tracking parameters, based on your network configuration.



**NOTE:** There is no shortcut to setting tracking parameters. The goals must first be set and the outcomes of various configurations and scenarios analyzed to find settings that meet the goals.

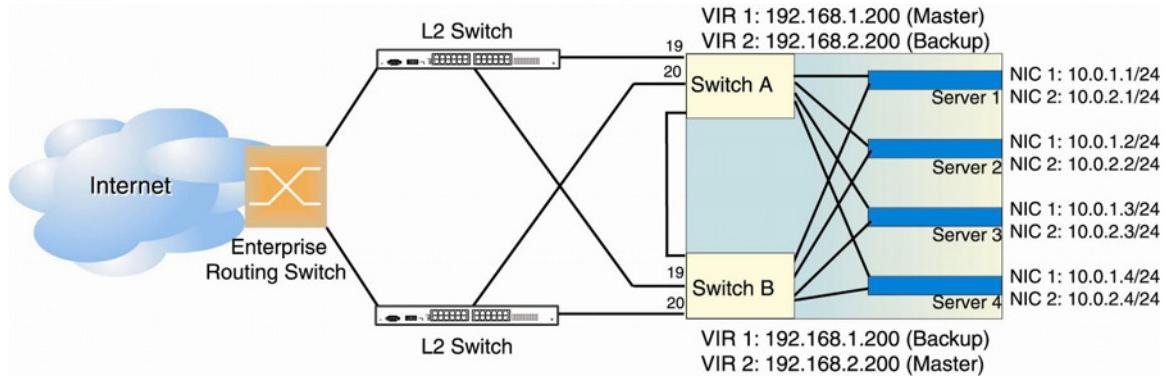
## High availability configurations

GbE2 Interconnect Switches offer flexibility in implementing redundant configurations. This section discusses the Active-Active configuration.

## Active-Active configuration

The following figure shows an example configuration, where two switches are used as VRRP routers in an active-active configuration. In this configuration, both switches respond to packets.

**Figure 27** Active-Active high availability configuration



Although this example shows only two switches, there is no limit on the number of switches used in a redundant configuration. It is possible to implement an active-active configuration across all the VRRP-capable switches in a LAN.

Each VRRP-capable switch in an active-active configuration is autonomous. Switches in a virtual router need not be identically configured.

In the scenario illustrated in the figure, traffic destined for IP address 10.0.1.1 is forwarded through the Layer 2 switch at the top of the drawing, and ingresses Switch A on port 19. Return traffic uses default gateway 1 (192.168.1.1). If the link between Switch A and the Layer 2 switch fails, Switch B becomes the Master because it has a higher priority. Traffic is forwarded to Switch B, which forwards it to Switch A through the crosslink (ports 17-18). Return traffic uses default gateway 2 (192.168.2.1), and is forwarded through the Layer 2 switch at the bottom of the drawing.

To implement the active-active example, perform the following switch configuration.

### Task 1: Configure Switch A

#### 1. Configure ports.

```
/cfg/l2/vlan 10          (Select VLAN 10)
>> VLAN 10# ena          (Enable VLAN 10)
>> VLAN 10# add 19       (Add port 19 to VLAN 10)
>> VLAN 10# ..
>> Layer 2# vlan 20      (Select VLAN 20)
>> VLAN 20# ena          (Enable VLAN 20)
>> VLAN 20# add 20       (Add port 20 to VLAN 20)
```

#### 2. Configure client and server interfaces.

```
/cfg/l3/if 1              (Select interface 1)
>> IP Interface 1# addr 192.168.1.100 (Define IP address for interface 1)
>> IP Interface 1# vlan 10   (Assign VLAN 10 to interface 1)
>> IP Interface 1# ena     (Enable interface 1)
>> IP Interface 1# ..
>> Layer 3# if 2          (Select interface 2)
>> IP Interface 2# addr 192.168.2.101 (Define IP address for interface 2)
>> IP Interface 1# vlan 20 (Assign VLAN 20 to interface 2)
>> IP Interface 2# ena     (Enable interface 2)
>> IP Interface 2# ..
>> Layer 3# if 3          (Select interface 3)
>> IP Interface 3# addr 10.0.1.100 (Define IP address for interface 3)
>> IP Interface 3# mask 255.255.255.0 (Define subnet mask for interface 3)
>> IP Interface 3# ena     (Enable interface 3)
>> IP Interface 2# ..
>> Layer 3# if 4          (Select interface 4)
>> IP Interface 4# addr 10.0.2.101 (Define IP address for interface 4)
>> IP Interface 4# mask 255.255.255.0 (Define subnet mask for interface 4)
>> IP Interface 4# ena     (Enable interface 4)
```

3. Configure the default gateways. Each default gateway points to one of the Layer 2 routers.

<pre>/cfg/13/gw 1 &gt;&gt; Default gateway 1# addr 192.168.1.1 &gt;&gt; Default gateway 1# ena &gt;&gt; Default gateway 1# .. &gt;&gt; Layer 3# gw 2 &gt;&gt; Default gateway 1# addr 192.168.2.1 &gt;&gt; Default gateway 1# ena</pre>	(Select default gateway 1) (Point gateway to the first L2 router) (Enable the default gateway)  (Select default gateway 2) (Point gateway to the second router) (Enable the default gateway)
---	--

4. Turn on VRRP and configure two Virtual Interface Routers.

<pre>/cfg/13/vrrp/on &gt;&gt; Virtual Router Redundancy Protocol# vr 1 &gt;&gt; VRRP Virtual Router 1# vrid 1 &gt;&gt; VRRP Virtual Router 1# if 1 &gt;&gt; VRRP Virtual Router 1# addr 192.168.1.200 &gt;&gt; VRRP Virtual Router 1# ena &gt;&gt; VRRP Virtual Router 1# .. &gt;&gt; Virtual Router Redundancy Protocol# vr 2 &gt;&gt; VRRP Virtual Router 2# vrid 2 &gt;&gt; VRRP Virtual Router 2# if 2 &gt;&gt; VRRP Virtual Router 2# addr 192.168.2.200 &gt;&gt; VRRP Virtual Router 2# ena</pre>	(Turn VRRP on) (Select virtual router 1) (Set VRID to 1) (Set interface 1) (Define IP address) (Enable virtual router 1) (Enable virtual router 1) (Select virtual router 2) (Set VRID to 2) (Set interface 2) (Define IP address) (Enable virtual router 2)
---	---

5. Enable tracking on ports. Set the priority of Virtual Router 1 to 101, so that it becomes the Master.

<pre>/cfg/13/vrrp/vr 1 &gt;&gt; VRRP Virtual Router 1# track/ports/ena &gt;&gt; VRRP Virtual Router 1 Priority Tracking# .. &gt;&gt; VRRP Virtual Router 1# prio 101 &gt;&gt; VRRP Virtual Router 1# .. &gt;&gt; Virtual Router Redundancy Protocol# vr 2 &gt;&gt; VRRP Virtual Router 1# track/ports/ena</pre>	(Select VRRP virtual router 1) (Set tracking on ports)  (Set the VRRP priority)  (Select VRRP virtual router 2) (Set tracking on ports)
---	---

6. Turn off Spanning Tree Protocol globally.

<pre>/cfg/12/stg 1/off &gt;&gt; Spanning Tree Group 1# apply &gt;&gt; Spanning Tree Group 1# save</pre>	(Turn off STG)
---	----------------

## Task 2: Configure Switch B

1. Configure ports.

<pre>/cfg/12/vlan 10 &gt;&gt; VLAN 10# ena &gt;&gt; VLAN 10# add 19 &gt;&gt; VLAN 10# .. &gt;&gt; Layer 2# vlan 20 &gt;&gt; VLAN 20# ena &gt;&gt; VLAN 20# add 20</pre>	(Select VLAN 10) (Enable VLAN 10) (Add port 19 to VLAN 10)  (Select VLAN 20) (Enable VLAN 20) (Add port 20 to VLAN 20)
---	--

2. Configure client and server interfaces.

<pre>/cfg/13/if 1 &gt;&gt; IP Interface 1# addr 192.168.1.101 &gt;&gt; IP Interface 1# vlan 10 &gt;&gt; IP Interface 1# ena &gt;&gt; IP Interface 1# .. &gt;&gt; Layer 3# if 2 &gt;&gt; IP Interface 2# addr 192.168.2.100 &gt;&gt; IP Interface 1# vlan 20 &gt;&gt; IP Interface 2# ena &gt;&gt; IP Interface 2# .. &gt;&gt; Layer 3# if 3 &gt;&gt; IP Interface 3# addr 10.0.1.101 &gt;&gt; IP Interface 3# mask 255.255.255.0 &gt;&gt; IP Interface 3# ena &gt;&gt; IP Interface 2# .. &gt;&gt; Layer 3# if 4 &gt;&gt; IP Interface 4# addr 10.0.2.100 &gt;&gt; IP Interface 4# mask 255.255.255.0 &gt;&gt; IP Interface 4# ena</pre>	(Select interface 1) (Define IP address for interface 1) (Assign VLAN 10 to interface 1) (Enable interface 1)  (Select interface 2) (Define IP address for interface 2) (Assign VLAN 20 to interface 2) (Enable interface 2)  (Select interface 3) (Define IP address for interface 3) (Define subnet mask for interface 3) (Enable interface 3)  (Select interface 4) (Define IP address for interface 4) (Define subnet mask for interface 4) (Enable interface 4)
--	--

3. Configure the default gateways. Each default gateway points to one of the Layer 2 routers.

```
/cfg/l3/gw 1          (Select default gateway 1)
>> Default gateway 1# addr 192.168.2.1 (Point gateway to the first L2 router)
>> Default gateway 1# ena                (Enable the default gateway)
>> Default gateway 1# ..
>> Layer 3# gw 2          (Select default gateway 2)
>> Default gateway 1# addr 192.168.1.1 (Point gateway to the second router)
>> Default gateway 1# ena                (Enable the default gateway)
```

4. Turn on VRRP and configure two Virtual Interface Routers.

```
/cfg/l3/vrrp/on          (Turn VRRP on)
>> Virtual Router Redundancy Protocol# vr 1 (Select virtual router 1)
>> VRRP Virtual Router 1# vrid 1           (Set VRID to 1)
>> VRRP Virtual Router 1# if 1            (Set interface 1)
>> VRRP Virtual Router 1# addr 192.168.1.200 (Define IP address)
>> VRRP Virtual Router 1# ena             (Enable virtual router 1)
>> VRRP Virtual Router 1# ..
>> VRRP Virtual Router 1# ..              (Enable virtual router 1)
>> Virtual Router Redundancy Protocol# vr 2 (Select virtual router 2)
>> VRRP Virtual Router 2# vrid 2           (Set VRID to 2)
>> VRRP Virtual Router 2# if 2            (Set interface 2)
>> VRRP Virtual Router 2# addr 192.168.2.200 (Define IP address)
>> VRRP Virtual Router 2# ena             (Enable virtual router 2)
```

5. Enable tracking on ports. Set the priority of Virtual Router 2 to 101, so that it becomes the Master.

```
/cfg/l3/vrrp/vr 1          (Select VRRP virtual router 1)
>> VRRP Virtual Router 1# track/ports/ena (Set tracking on ports)
>> VRRP Virtual Router 1 Priority Tracking# ..
>> VRRP Virtual Router 1# ..
>> Virtual Router Redundancy Protocol# vr 2 (Select VRRP virtual router 2)
>> VRRP Virtual Router 2# track/ports/ena (Set tracking on ports)
>> VRRP Virtual Router 2 Priority Tracking# ..
>> VRRP Virtual Router 2# prio 101        (Set the VRRP priority)
```

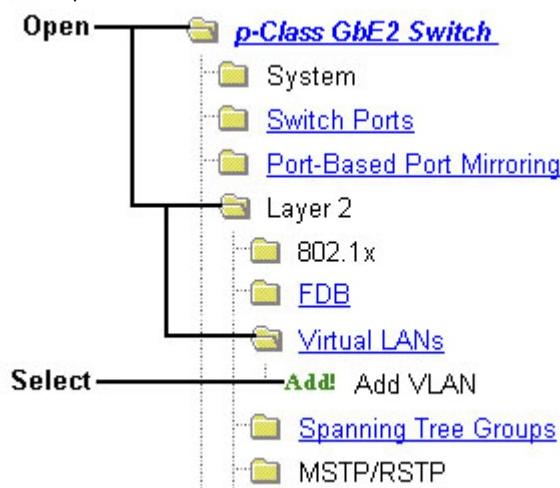
6. Turn off Spanning Tree Protocol globally. Apply and save changes.

```
/cfg/l2/stg 1/off          (Turn off STG)
>> Spanning Tree Group 1# apply
>> Spanning Tree Group 1# save
```

## Task 1: Configure Switch A (BBI example)

1. Configure ports and VLANs.

- Click the **Configure** context button.
- Open the Virtual LANs folder, and select **Add VLAN**.



- c. Configure port 19 as a member of VLAN 10 and port 20 as a member of VLAN 20. Enable each VLAN.

**VLAN "New" Configuration**

VLAN Name	VLAN Ten
VLAN ID (1 - 4095) From	10
VLAN State	enabled
Spanning Tree Group	1

Ports Available	Ports in Vlan
<div style="border: 1px solid #ccc; padding: 5px; width: 100%;"> Port:15  Port:16  Port:17  Port:18  Port:20  Port:21  Port:22  Port:23  Port:24 </div>	<div style="border: 1px solid #ccc; padding: 5px; width: 100%;"> <span style="border: 1px solid #ccc; padding: 2px;">Add&gt;&gt;</span>    <span style="border: 1px solid #ccc; padding: 2px;">&lt;&lt;Remove</span> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px; background-color: #000; color: white; text-align: center; width: fit-content;"> Port ID Port:19 </div> </div>

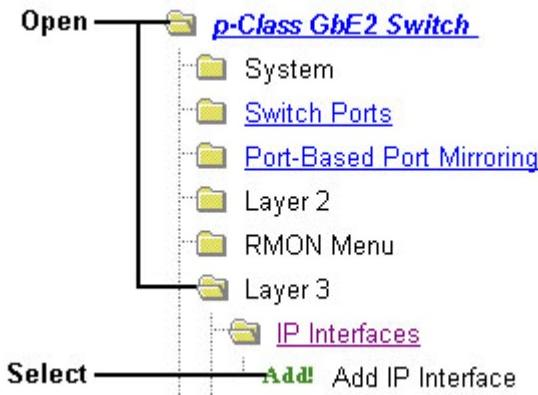
  

d. Click **Submit**.

2. Configure the following client and server interfaces:

- IF 1  
IP address = 192.168.1.100  
Subnet mask = 255.255.255.0  
VLAN 10
- IF 2  
IP address = 10.10.12.1  
Subnet mask = 255.255.255.0  
VLAN 20
- IF 3  
IP address = 10.10.12.1  
Subnet mask = 255.255.255.0
- IF 4  
IP address = 10.10.12.1  
Subnet mask = 255.255.255.0

- a. Open the IP Interfaces folder, and select **Add IP Interface**.



- b. Configure an IP interface. Enter the IP address, subnet mask, and VLAN membership. Enable the interface.

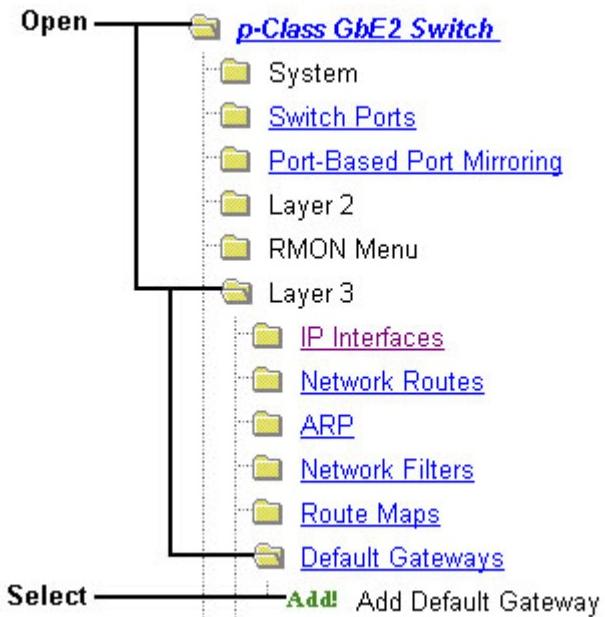
### IP Interface Configuration

IP Interface Identifier (1-255)	1
IP Address	192.168.1.100
Enabled?	<input checked="" type="checkbox"/>
Subnet Mask	255.255.255.0
Broadcast Address	
VLAN Membership ID (1 - 4095)	10
Enable/Disable BOOTP Relay	<input checked="" type="checkbox"/>

- c. Click **Submit**.

3. Configure the default gateways. Each default gateway points to one of the Layer 2 routers.

- a. Open the Default Gateways folder, and select **Add Default Gateway**.



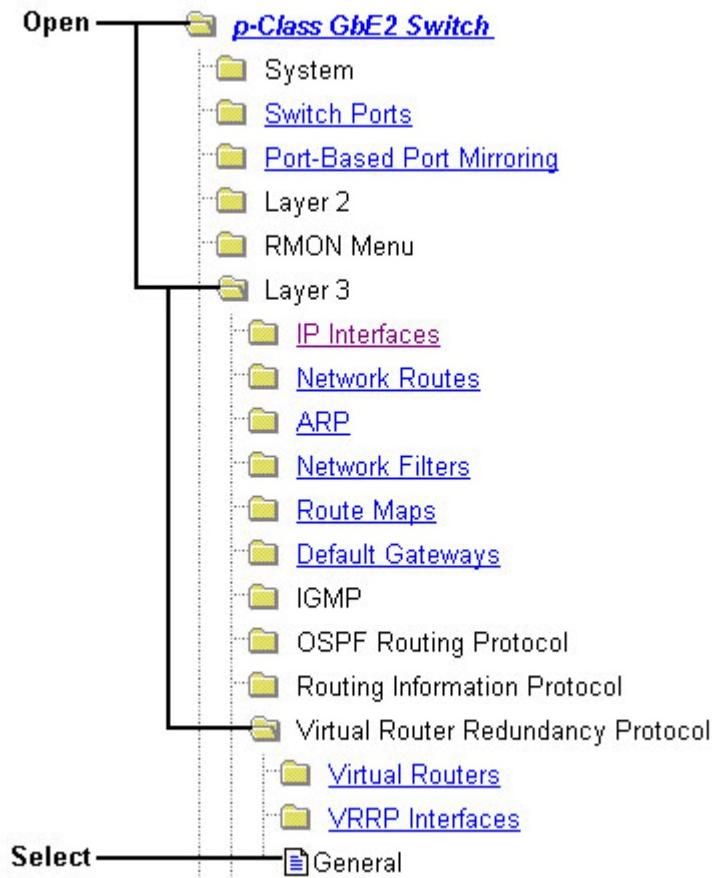
- b. Configure the IP address for each default gateway. Enable the default gateways.

**Default Gateway Configuration**

Default Gateway Identifier(1 - 4)	<input type="text" value="1"/>
Default Gateway IP Address	<input type="text" value="192.168.1.1"/>
Enable/Disable Default Gateway	<input type="button" value="Enabled"/>
Enable/Disable ARP only health checks	<input type="button" value="Disabled"/>
Health Check Interval (0-60 sec)	<input type="text" value="2"/>
Retries before Out of Service (1-120)	<input type="text" value="8"/>

- c. Click **Submit**.

4. Turn on VRRP and configure two Virtual Interface routers.
- a. Open the Virtual Router Redundancy Protocol folder, and select **General**.



- b. Enable VRRP processing.

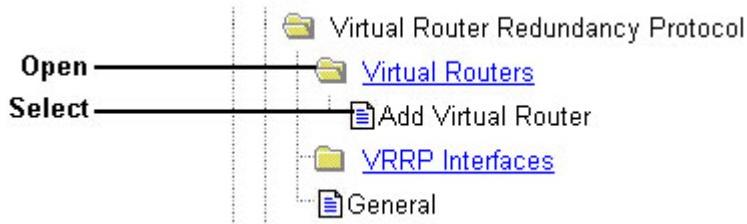
VRRP General Configuration	
VRRP Processing Enabled?	<input type="button" value="Enabled"/>
VRRP virtual router tracking increment (0-254)	2
VRRP IP interface tracking increment (0-254)	2
VRRP VLAN switch port tracking increment (0-254)	2

VRRP Virtual Router Group Configuration	
Virtual Router Identifier (1- 255)	1
Enabled?	<input type="button" value="Disabled"/>
Advertisement Interval(1- 255)	1
Track other IP interfaces?	<input type="button" value="Disabled"/>
IP interface (1- 255)	1
Priority (1- 254)	100
Owner Preemption?	<input type="button" value="Enabled"/>
Track master virtual routers?	<input type="button" value="Disabled"/>
Track VLAN switch ports?	<input type="button" value="Disabled"/>

c. Click **Submit**.

d. Open the Virtual Routers folder, and select **Add Virtual Router**.



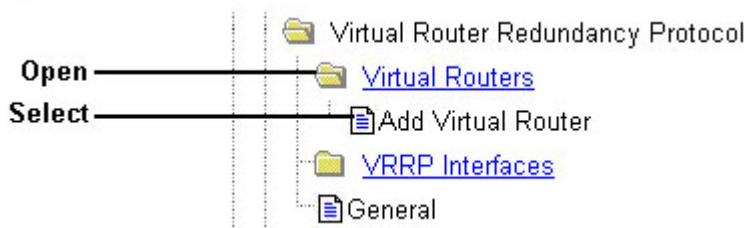
- e. Configure the IP address for Virtual Router 1 (VR1). Enable tracking on ports, and set the priority to 101. Enable The Virtual Router.

**Virtual Router Configuration**

Virtual Router Number (1- 255)	1
Virtual Router Identifier (1- 255)	1
IP Address	192.168.1.200
IP interface (1-254)	1
Enabled?	Enabled ▾
Priority (1- 254)	101
Advertisement Interval (1- 255)	1
Owner Preemption?	Enabled ▾
Track master virtual routers?	Disabled ▾
Track other IP interfaces?	Disabled ▾
Track VLAN switch ports?	Enabled ▾

Submit      Delete

- f. Click **Submit**.  
g. Select Add Virtual Router.



- h. Configure the IP address for Virtual Router 2 (VR2). Enable tracking on ports, but set the priority to 100 (default value). Enable The Virtual Router.

**Virtual Router Configuration**

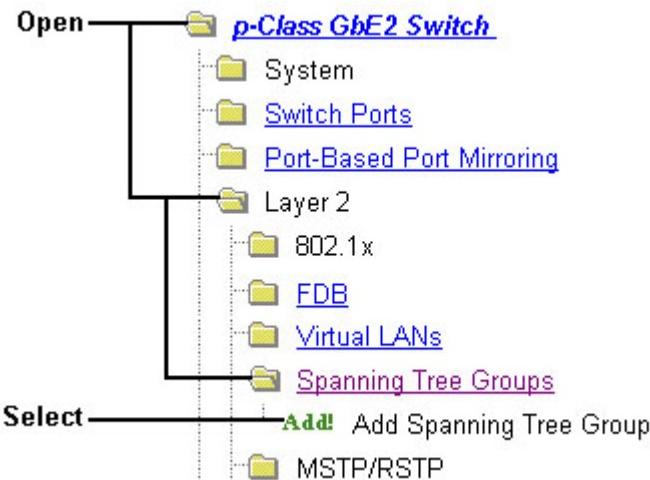
Virtual Router Number (1- 255)	2
Virtual Router Identifier (1- 255)	2
IP Address	192.168.2.200
IP interface (1-254)	2
Enabled?	Enabled
Priority (1- 254)	100
Advertisement Interval (1- 255)	1
Owner Preemption?	Enabled
Track master virtual routers?	Disabled
Track other IP interfaces?	Disabled
Track VLAN switch ports?	Enabled

**Submit**    **Delete**

i. Click **Submit**.

5. Turn off Spanning Tree globally.

a. Open the Spanning Tree Groups folder, and select **Add Spanning Tree Group**.



- b. Enter Spanning Tree Group ID 1 and set the Switch Spanning Tree State to off.

### Switch Spanning Tree Group Configuration

Spanning Tree Group ID (1-32)	2
Switch Spanning Tree State	<input style="width: 100%; height: 100%;" type="button" value="off"/>
Bridge Priority (0-65535)	32768
Bridge Hello Time (1-10secs)	2
Bridge Max Age (6-40secs)	20
Bridge Forward Delay (4-30secs)	15

**VLANs Available**

Vlan ID:Name  
1:Default VLAN  
100:UplinkVLAN  
134:VLAN 134

**VLANs in STG**

Vlan ID:Name

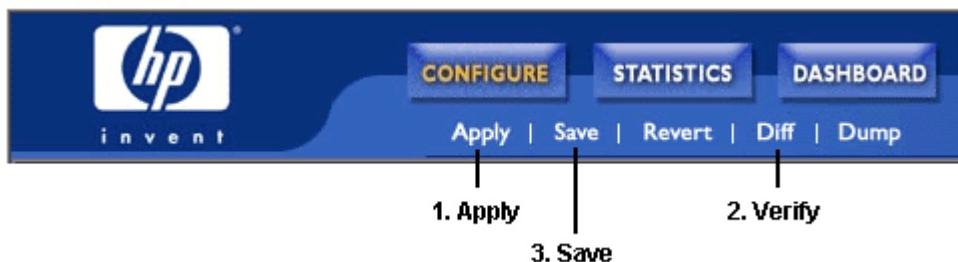
  

### Switch Spanning Tree Port Configuration

Switch Port	Port Priority	Port Path Cost	Port Spanning Tree State
<u>1</u>	128	4	off
<u>2</u>	128	4	off

c. Click Submit.

6. Apply, verify, and save the configuration.



# Troubleshooting tools

## Introduction

This appendix discusses some tools to help you use the Port Mirroring feature to troubleshoot common network problems on the HP ProLiant BL p-Class GbE2 Interconnect Switch.

## Port Mirroring

The Port Mirroring feature on the GbE2 Interconnect Switch is very useful for troubleshooting any connection-oriented problem. Any traffic in or out of one or more ports can be mirrored to a single monitoring port to which a network monitor can be attached.

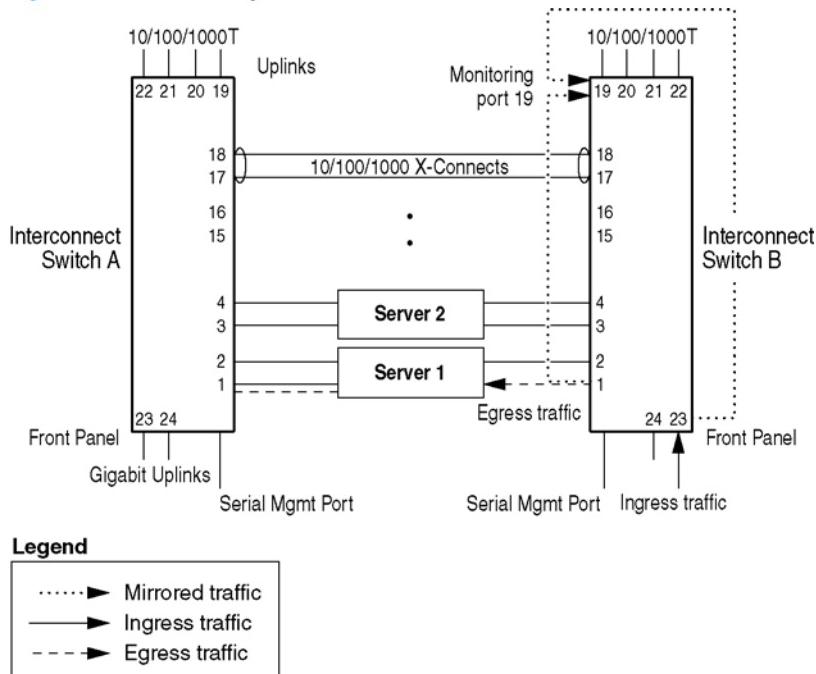
Port Mirroring can be used as a troubleshooting tool or to enhance the security of your network. For example, an Intrusion Detection Service (IDS) server can be connected to the monitor port to detect intruders attacking the network.



**NOTE:** The monitor port must be in the same VLAN as the mirrored port to ensure Port Mirroring works correctly.

As shown in the following figure, port 19 is monitoring ingress traffic (traffic entering the GbE2 Interconnect Switch) on port 23 and egress traffic (traffic leaving the GbE2 Interconnect Switch) on port 1. You can attach a device to port 19 to monitor the traffic on ports 23 and 1.

**Figure 28** Port Mirroring



This figure shows two mirrored ports monitored by a single port. Similarly, you can have one mirrored port to one monitored port, or many mirrored ports to one monitored port. The GbE2 Interconnect Switch does not support a single port being monitored by multiple ports because it supports only one monitored port configured at a time.

Ingress traffic is duplicated and sent to the mirrored port before processing, and egress traffic is duplicated and sent to the mirrored port after processing.

## Configuring Port Mirroring (CLI example)

To configure Port Mirroring for the example shown in the preceding figure:

1. Specify the monitoring port.

```
>> # /cfg/pmirr/monport 19 (Select port 19 for monitoring)
```

2. Select the ports that you want to mirror.

```
>> Port 19 # add 23 (Select port 23 to mirror)
```

```
>> Enter port mirror direction [in, out, or both]: in  
(Monitor ingress traffic on port 23)
```

```
>> Port 19 # add 11 (Select port 11 to mirror)
```

```
>> Enter port mirror direction [in, out, or both]: out  
(Monitor egress traffic on port 1)
```

3. Enable Port Mirroring.

```
>> # /cfg/pmirr/mirr ena (Enable port mirroring)
```

4. Apply and save the configuration.

```
>> PortMirroring# apply (Apply the configuration)
```

```
>> PortMirroring# save (Save the configuration)
```

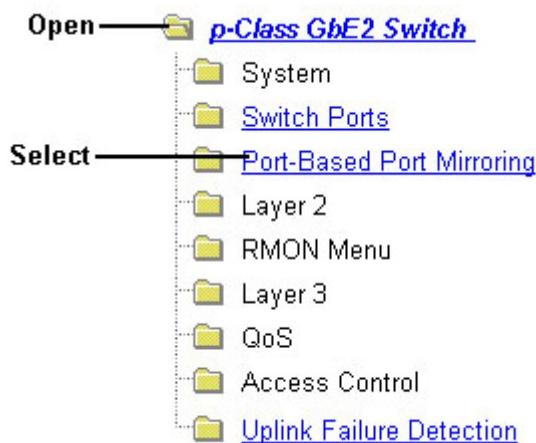
5. View the current configuration.

```
>> PortMirroring# cur (Display the current settings)
```

```
Port mirroring is enabled  
Monitoring Ports Mirrored Ports  
1none  
2none  
3none  
4none  
5none  
:  
:  
17none  
18none  
19(23, in) (11, out)  
20none  
:
```

## Configuring Port Mirroring (BBI example)

1. Configure Port Mirroring.
  - a. Click the **Configure** context button.
  - b. Open the Switch folder, and select **Port-Based Port Mirroring** (click the underlined text, not the folder).



- c. Click a port number to select a monitoring port.

**Port-Based Port Mirroring Configuration**

Enable Port-Based Port Mirroring?

**Port Mirroring Table**

Monitoring Port	Mirrored Ports
<a href="#">1</a>	none
<a href="#">2</a>	none
<a href="#">3</a>	none
<a href="#">4</a>	none
<a href="#">5</a>	none
<a href="#">6</a>	none
<a href="#">7</a>	none
<a href="#">8</a>	none
<a href="#">9</a>	none
<a href="#">10</a>	none
<a href="#">11</a>	none
<a href="#">12</a>	none
<a href="#">13</a>	none
<a href="#">14</a>	none
<a href="#">15</a>	none
<a href="#">16</a>	none
<a href="#">17</a>	none
<a href="#">18</a>	none
<a href="#">19</a>	none
<a href="#">20</a>	none

Select ——  [19](#)

- d. Click Add Mirrored Port.

**Monitoring Port 19 Configuration**

Mirrored Port	Direction
<a href="#">Add Mirrored Port</a>	

- e. Enter a port number for the mirrored port, and select the Port Mirror Direction.

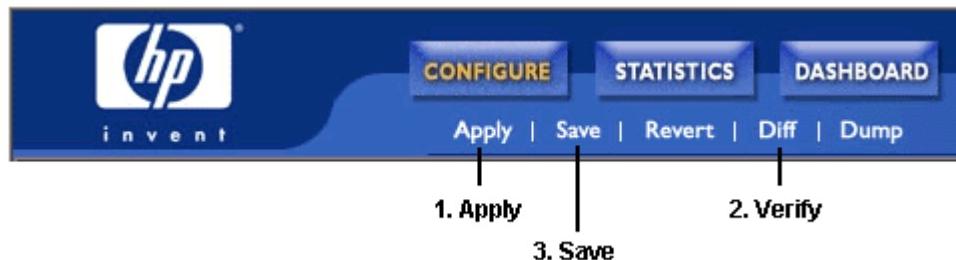
**Port Mirroring Configuration for Port 19**

Mirrored Port	23
Port Mirror Direction	In

**Submit**   **Delete**

- f. Click **Submit**.

2. Apply, verify, and save the configuration.



3. Verify the Port-Mirroring information on the switch.

**Monitoring Port 19 Configuration**

Mirrored Port	Direction
<a href="#">11</a>	out
<a href="#">23</a>	in

[Add Mirrored Port](#)

# Other network troubleshooting techniques

Other network troubleshooting techniques include the following.

## Console and Syslog messages

When a GbE2 Interconnect Switch experiences a problem, review the console and Syslog messages. The GbE2 Interconnect Switch displays these informative messages when state changes and system problems occur. Syslog messages can be viewed by using the /info/sys/log command. For more information on interpreting syslog messages, see the *HP ProLiant BL p-Class GbE2 Interconnect Switch Command Reference Guide*.

## Ping

To verify station-to-station connectivity across the network, execute the following command:

```
ping <host name> | <IP address> [ (number of tries)> [ msec delay ] ]
```

The IP address is the hostname or IP address of the device. The number of tries (optional) is the number of attempts (1-32). Msec delay (optional) is the number of milliseconds between attempts.

## Trace route

To identify the route used for station-to-station connectivity across the network, execute the following command:

```
traceroute <host name> | <IP address> [<max-hops> [ msec delay ] ]
```

The IP address is the hostname or IP address of the target station. Max-hops (optional) is the maximum distance to trace (1-16 devices). Msec delay (optional) is the number of milliseconds to wait for the response.

## Statistics and state information

The GbE2 Interconnect Switch keeps track of a large number of statistics and many of these are error condition counters. The statistics and state information can be very useful when troubleshooting a LAN or Real Server problem. For more information about available statistics, see one of the following:

- "Viewing statistics" chapter of the *HP ProLiant BL p-Class GbE2 Interconnect Switch Browser-based Interface Reference Guide*, or
- "Statistics Menu" chapter of the *HP ProLiant BL p-Class GbE2 Interconnect Switch Command Reference Guide*
- "Statistics Commands" chapter of the *HP ProLiant BL p-Class GbE2 Interconnect Switch ISCLI Reference Guide*

## Customer support tools

The following diagnostics tools are not user-configurable and should be performed through HP technical support.

- Offline Diagnostics—this tool is used for troubleshooting suspected GbE2 Interconnect Switch hardware issues. These tests verify that the selected hardware is performing within expected engineering specifications.
- Software Panics—if a fatal software condition is found during runtime, the GbE2 Interconnect Switch will capture the current hardware and software state information into a panic dump. This dump file can be analyzed post-mortem to determine the cause of the problem.
- Stack Trace—if a fatal software condition occurs, the GbE2 Interconnect Switch dumps stack trace data to the console. If you have a console attached to the switch, capture the console dump, and forward it to HP technical support.

# Index

## 8

802.1x port states, 42

## A

accessing the switch: defining source IP addresses, 16; RADIUS authentication, 16; security, 16; using the command line interface (CLI), 9  
ACL Blocks and Groups, 75  
ACL configuration examples, 78  
ACL filters, 74  
active-active redundancy, 150  
allowable source IP addresses, 16

## B

BBI: See Browser-Based Interface, 114  
Bridge Protocol Data Unit (BPDU), 57  
broadcast domains, 45, 49  
Browser-Based Interface, 114

## C

Cisco EtherChannel, 32  
Class of Service queueCOS queue, 89  
Command Line Interface, 114  
command line interface (CLI), 9  
configuration, 32  
configuration rules: port mirroring, 32; trunking, 32; VLANs, 32  
configuring: OSPF, 120  
configuring SNMP trap hosts, 14  
console messages, 167  
console port, 9  
customer support tools, 167

## D

default gateway: configuration example, 10, 93  
Differentiated Services Code Point (DSCP)DSCP, 82  
Dynamic Host Configuration Protocol, 95

## E

EAPoL configuration guidelines, 43  
EtherChannel, as used with port trunking, 32  
Extensible Authentication Protocol over LAN (EAPoL)EAPoL, 40

## F

switch failover: overview, 149  
Fast Uplink Convergence, 63  
fault tolerance, port trunking, 31  
FDB static entries, 56  
frame tagging, 46

## G

default gateway, 91

## H

high-availability, 8, 143  
Hot Links, 63

## I

IBM DirectorSNMP: IBM Director, 11  
IEEE 802.1Q VLAN tagging, 46, 49  
IEEE standards: 802.1x, 40  
IGMP Filtering, configuring (BBI example), 106  
IGMP Filtering, configuring (CLI example), 102  
IGMP Snooping, 100  
IGMP Snooping, configuring (BBI example), 104  
IGMP Snooping, configuring (CLI example), 101  
IP address: routing example, 92  
IP interfaces: configuring, 9; example configuration, IP interface configuration, 94; VLAN #1 (default), 49; VLANs, 49  
IP routing, 90; default gateway configuration, 10, 93; IP interface configuration, 92, 94; IP interfaces example configuration, 92  
IP subnets: routing; IP subnets, 91; routing, 91  
IP subnets, VLANs, 45

## J

fragmenting jumbo frames: fragmenting to normal size; routing, 90

## L

LACP, 37  
Link Aggregation Control Protocol, 37  
logical segment, 45  
LSAs, 113

## M

Main Menu, command line interface (CLI), 9  
media access control (MAC) address, 9  
meter, 77  
mirroring ports, 163  
monitoring ports, 163  
MSTP, 65  
multi-links between switches, using port trunking, 30  
multiple spanning tree groups, 59

## N

network management, 11

## O

Open Shortest Path First (OSPF), 111  
ICMP;IGMP;TCP;UDP: filtering criteria, 74  
OSPF: overview, 111  
OSPF: area types, 111  
OSPF: neighbors, 113  
OSPF: link state database, 113  
OSPF: route summarization, 116  
OSPF: default route; OSPF, 117  
OSPF: virtual link, 117  
OSPF: authentication, 118  
OSPF: host routes; OSPF, 119  
OSPF: external routes, 120  
OSPF configuration examples, 120, 122, 128, 130, 131  
OSPF configuration, verifying, 132

## P

ping, 167  
Port Fast Forwarding, 62  
port mirroring: configuration rules, 32; troubleshooting, 163  
port trunking, 31  
port trunking, fault tolerance, 31  
Port-based Network Access control, 40  
Port-based traffic control, 43  
ports: monitoring, 163; physical, 46  
priority value (802.1p), 83  
PVID (port VLAN ID), 45

## Q

Quality of Service, 73  
queuing and scheduling, 89

## R

RADIUS: port 1812 and 1645, 75; port 1813, 75  
redundancy: active-active, 150; VRRP (Virtual Router Redundancy Protocol), 150  
re-mark, 77  
Remote Authentication Dial-in User Service (RADIUS): authentication, 16; SSH/SCP, 28  
Remote monitoring (RMON), 133  
RIP (Routing Information Protocol): advertisements, 97; distance vector protocol, 97; hop count, 97; metric, 97; TCP/IP route information, 8, 97  
RIP configuration, example, 99  
RIP features, 98  
RMON (remote monitoring), 133  
RMON groups: alarms, 137; events, 141; examples of, 133, 134, 136, 137, 138, 139, 140, 141, 145; history, 136; statistics, 133  
Router ID: OSPF; router ID, 118  
routers, 91, 93; border; peer; autonomous systems (AS), 113; switch-based routing topology, 91  
routing: internal and external; internal routing, 113  
Routing Information Protocol. See RIP, 97  
RSA keys, 28  
RSTP, 65

## S

security, 16; RADIUS authentication, 16; switch management, 16; VLANs, 45  
segmentation, 45  
HP-OpenView: HP-OpenView, 11  
SNMP, 11  
SNMP, 114  
SNMP v1.0, 11  
SNMP v3.0, 11  
Spanning Tree Protocol (STP), multiple instances, 60  
spanning tree, configuration rules, 32  
SSH: RSA host and server keys, 28; supported clients, 25  
SSH/SCP configuring, 26  
Static MRouter, configuring (CLI example), 103  
Static Multicast Router, configuring (BBI example), 109  
statistics, 167  
switch management: security, 16; via IP interface, 49  
switch ports VLANs membership, 46  
syslog messages, 167

## T

tagging, 46  
technical terms: port VLAN identifier (PVID), 46; tagged frame, 46; tagged member, 46; untagged

frame, 46; untagged member, 46; VLAN identifier (VID), 46

Telnet, 10

trace route, 167

Trunk Hash algorithm, 37

trunking: configuration rules, 32

typographical conventions, 9

## U

UDP: jumbo frame traffic

fragmentation; fragmenting jumbo frames; fragmenting to normal size; routing, 91

## V

VLANs: broadcast domains, 45, 49, 93; configuration rules, 32; default PVID, 45; example showing multiple VLANs, 49; ID numbers, 45; IP interface configuration, 94; IP interfaces, 49; multiple spanning trees, 57; multiple VLANs, 46; port members, 46; PVID, 45; security, 45; Spanning-Tree Protocol, 57; tagging, 46; topologies, 49; VLAN #1 (default), 49

VRRP (Virtual Router Redundancy Protocol): active-active redundancy, 150; overview, 148; virtual router ID numbering; ID numbering, 151; overview; tracking, 150; vrid, 148